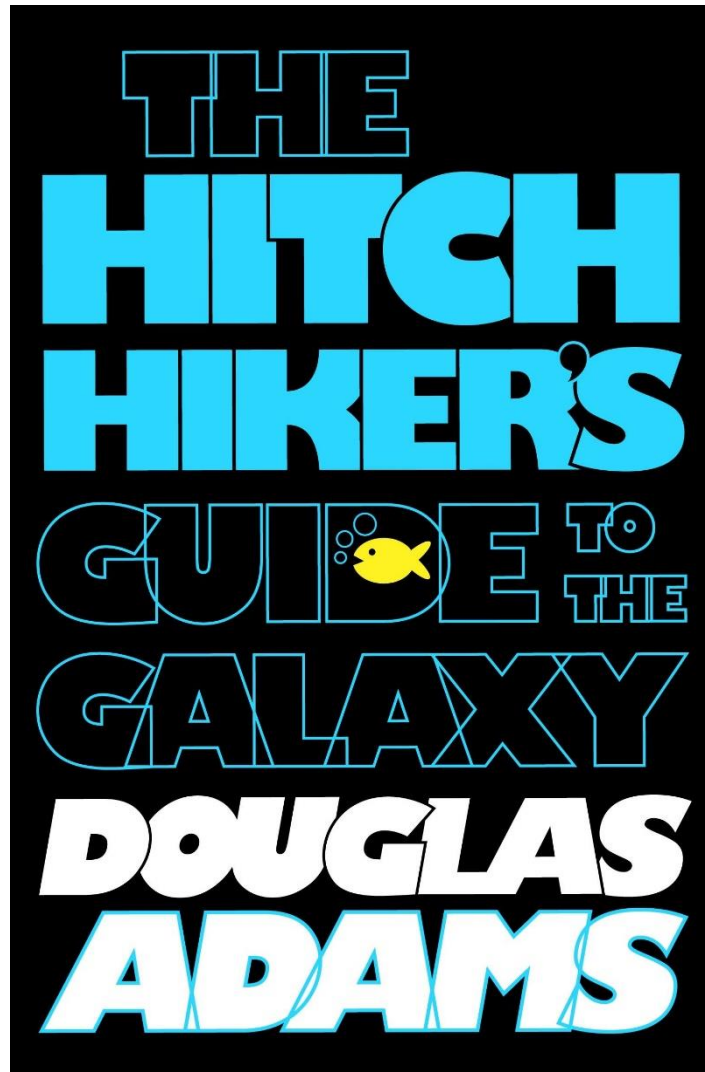


# Internet (in)security

Levente Buttyán

CrySyS Lab, BME

[www.crysys.hu](http://www.crysys.hu)





"If you're a researcher on this book thing and you were on Earth, you must have been gathering material on it."

"Well, I was able to extend the original entry a bit, yes."

"Let me see what it says in this edition, then. I've got to see it."

... "What? *Harmless*! Is that all it's got to say? *Harmless*! One word!

... Well, for God's sake I hope you managed to rectify that a bit."

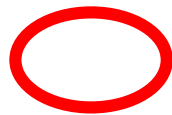
"Oh yes, well I managed to transmit a new entry off to the editor. He had to trim it a bit, but it's still an improvement."

"And what does it say now?" asked Arthur.

"*Mostly harmless*," admitted Ford with a slightly embarrassed cough.

# The Internet Is Broken

The Net's basic flaws cost firms billions, impede innovation, and threaten national security. It's time for a clean-slate app



**technology**  
**review**

Published by MIT



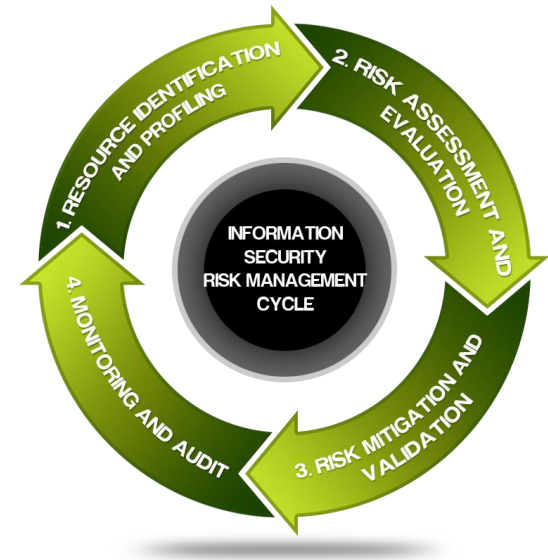
still

# The Internet Is Broken

The Net's basic flaws cost firms billions, impede innovation, and threaten national security. It's time for a clean-slate app

**2018**

By David Talbot on February 15, ~~2000~~



# WHAT IS IT SECURITY?

- security = management of risk
- IT security is about the management of risk resulting from
  - the loss of **confidentiality, integrity, or availability (CIA) of information** that is processed, stored, and transferred by IT systems
  - the **unauthorized access, corruption, or denial of services and resources** that are provided by IT systems

**IMPORTANT**

completely preventing such incidents is not possible in general

→ the goal should be to "**minimize**" the risk of getting compromised

# Safety vs. security

- both try to optimize the risk resulting from undesirable conditions, but ...
- **safety** focuses on risk resulting from random failures, accidents, and natural disasters
- **security** focuses on risk resulting from deliberate attacks carried out by intelligent attackers (malice)



safety



security



$$\text{Risk} = \text{Likelihood} \times \text{Impact}$$

(of attacks)

factors affecting risk:

- threats – people or entities who can do you harm (a.k.a. *attackers*)
  - » skill level, motive, opportunity, resources, ...
- vulnerabilities – weaknesses that allow for successful attacks
  - » ease of discovery, ease of exploit, awareness, ...
- potential loss – the loss you may experience
  - » nature of loss, business impact
- countermeasures – precautions you take
  - » technical and non-technical

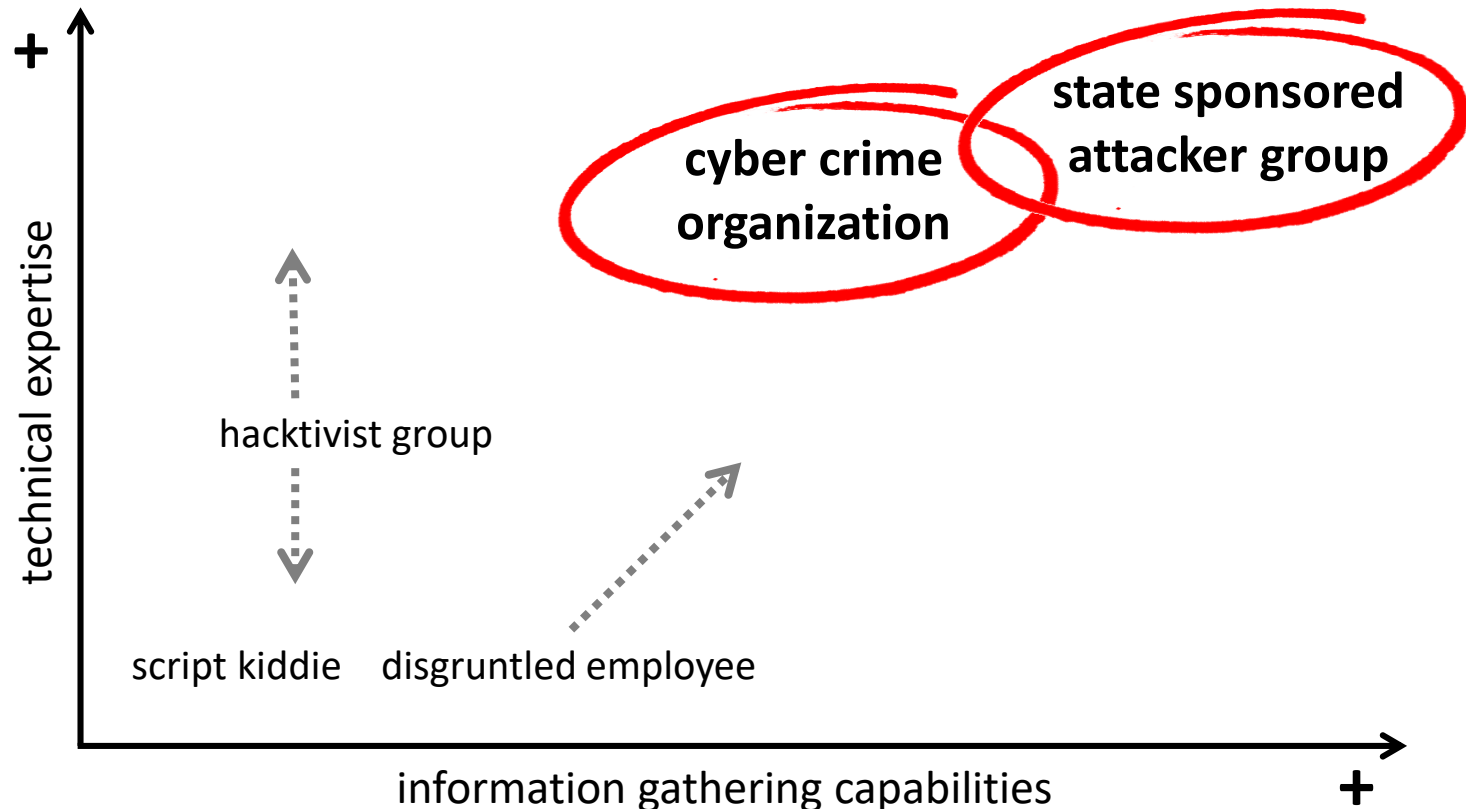
# Threats (attackers)

“If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.”

— Sun Tzu, *The Art of War*

# Threats (attackers)

- attackers differ in their motivation and goals, technical background, information gathering capabilities, and available resources



# Vulnerabilities

- four different types:
  - **technical:** design flaws and implementation errors in systems, hardware, software, and protocols
  - **physical:** weaknesses allowing for physical access (e.g., unlocked door)
  - **operational:** weaknesses in the procedures used to operate the system
  - **personnel:** related to security awareness and trustworthiness of people (e.g., employees, operators, contractors, ...)
- reasons for the existence of technical vulnerabilities
  - systems are designed, implemented, and operated by humans
    - » humans are imperfect and sometimes irrational
  - systems are increasingly complex
    - » easy to overlook flaws and mistakes (both in design and implementation)
    - » hard to test and reason about system properties
  - business constraints
    - » pressure on development time (reduce time-to-market)
    - » limited resources (budget, work force)
    - » functionality vs. security trade-offs

# Vulnerabilities

## all vulnerabilities

**known vulnerabilities –**  
vulnerabilities that have been  
identified by someone

**zero-day vulnerabilities –**  
vulnerabilities that are known  
only to potential attackers

**publicly known vulnerabilities –**  
vulnerabilities that have been  
made public

# Vulnerability management

- reported technical vulnerabilities get a globally recognized identifier
  - CVE ID – Common Vulnerabilities and Exposures ([cve.mitre.org](https://cve.mitre.org))
- information on reported technical vulnerabilities is stored in public vulnerability databases
  - structured vulnerability information in a searchable form
    - » technical details and descriptions, affected systems, impact, references to advisories, solutions, and tools
  - examples: US National Vulnerability Database ([nvd.nist.gov](https://nvd.nist.gov))
- public availability of vulnerability information helps keeping systems free from, at least, known vulnerabilities
  - this alone can dramatically decrease the risk one faces
  - on the other hand, there may be systems where fixing known vulnerabilities is slow or even impossible
    - » introducing patches requires extensive testing or needs special authorizations
    - » but at least you can count with those vulnerabilities when calculating the risk

# Zero-day vulnerabilities

- represent great advantage (hence value) for attackers
  - exploitable by definition!
- they are hard to find (or expensive to buy)
  - some companies make their living out of finding and selling zero-day vulnerabilities (or exploits) to criminals and governments
    - » Zerodium ([www.zerodium.com](http://www.zerodium.com))
    - » ReVuln ([revuln.com](http://revuln.com))
- typically used in targeted attacks
  - successfully compromising a particular target is important
  - risk of detection and exposure of the zero-day vulnerability is small
    - » if a zero-day vuln is exposed it becomes publicly known and gets fixed  
→ substantial loss for attackers

# Zero-day vulnerabilities

- what do they mean for the defender?
  - zero-day vulnerabilities are not counted in the risk equation!
    - » you are optimizing your system defences for the wrong objective ☹
  - could they be counted in somehow?
    - » how to estimate their likelihood?
    - » how to determine the impact of an unknown attack?
    - » what countermeasures should you apply against an unknown vulnerability?
  - is this a lost game for defenders???
- approaches to address the problem of zero-days
  - increase effectiveness of hunting zero-days in general
    - » bug bounty programs (The Internet Bug Bounty, Google VRP)
    - » open source software movement
  - decrease impact of zero-days on your system
    - » avoid single points of failure
    - » apply defence-in-depth architectures and strategies



# Countermeasures

- four different types:
  - **technical:** host and network security controls
    - » e.g., firewalls, anti-virus software, authentication tokens, security protocols, cryptographic algorithms, ...
  - **physical:** provide physical security
    - » e.g., locks, fences, security guards, tamper resistant hardware, ...
  - **operational:** policies and procedures related to the operation of the system and management of the personnel
    - » e.g., access control policies, password changing policies, key management procedures, regular security testing, ...
    - » e.g., hiring and firing procedures, separation of duties, vacation policies, ...
  - **personnel:** increase security awareness and trustworthiness of people
    - » e.g., security education, increasing employee satisfaction

# Risk minimization vs. risk optimization

- we said the goal of security is to “minimize” the risk of attacks
  - where risk was defined as the likelihood of attacks multiplied with their impact
- however, the goal is actually not risk minimization in an absolute sense
  - that would require to remove as much risk as possible, no matter the costs
- rather, we want to optimize risk, by which we mean minimizing it under some budget constraint
  - what are the plausible threats?
  - what are the known vulnerabilities?
  - what is the likelihood of those vulnerabilities being exploited by plausible threats?
  - what is the expected loss? (likelihood of attacks combined with the potentially resulting loss)
  - which countermeasures can reduce the expected loss in a cost effective way?



FreakingNews.com

# CYBERCRIME

# Cybercrime is a problem

cybercrime = crime that involves computers and networks

- computers can be used as tools or they can be the target
- examples: identity theft, phishing, spam, DDoS, ransomware, ...



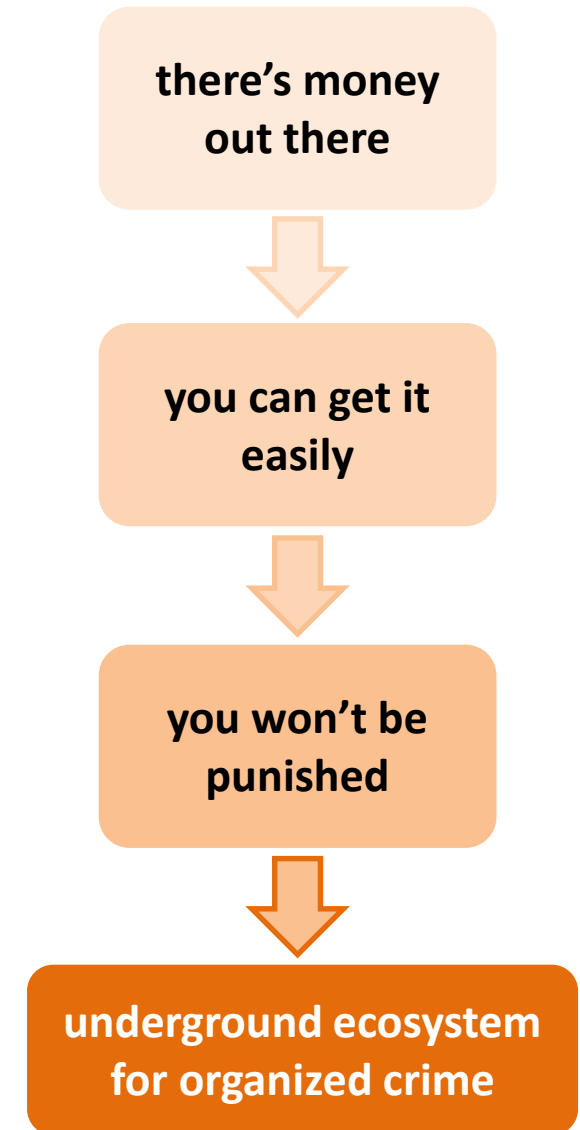
## 2017 Cybercrime Report

Cybercrime damages will cost the world  
\$6 trillion annually by 2021.

Steve Morgan, Editor-in-Chief  
Cybersecurity Ventures

# What makes cybercrime possible?

- large amount of valuable resources are available on the Internet
  - real and virtual money, data, services, computing resources
- plenty of exploitable weaknesses
  - poorly maintained systems
  - confused users with low level of security awareness
- laws and regulations are ill-defined and hard to enforce
  - cybercrime is global (international)
  - legal system is lagging behind



# The cyber underground

- largest underground economy in the world fostered by the Internet
- different actors that collaborate and trade with each other
  - specialized roles (resource dealers, service providers, tool makers, money mules, program managers)
  - mutual benefits (win-win situations, non-zero sum games)
- communication infrastructure
  - in the old days: IRC (Internet Relay Chat) networks
  - today: social networks and public forums
  - anonymous communication systems (e.g., Tor)
- products and services are sold and bought on underground markets
  - on-line interactions using various communication infrastructure
  - anonymous payment methods such as WU, e-gold, or bitcoin

# Underground market prices

Russian Cybercriminal Underground Market Product Offerings			
Product	2011 Price	2012 Price	2013 Price
Credit card credentials (per card): <ul style="list-style-type: none"><li>• American</li><li>• Australian</li><li>• Canadian</li><li>• German</li><li>• British</li></ul>	US\$2.50 US\$7 US\$5 US\$9 US\$7	US\$1 US\$5 US\$5 US\$7 US\$6–8	US\$1 US\$4 US\$4 US\$6 US\$5
Scanned fake document: <ul style="list-style-type: none"><li>• European passport</li><li>• Russian and other CIS passports</li></ul>	US\$2.50 US\$2–5	US\$1 US\$1–5	US\$1 US\$1–2

# Underground market prices

Russian Cybercriminal Underground Market Product Offerings			
Product	2011 Price	2012 Price	2013 Price
Trojan: <ul style="list-style-type: none"> <li>Phoenix</li> <li>Adrenalin</li> <li>Limbo</li> <li>Zeus (detected by Trend Micro as "ZBOT")</li> <li>SpyEye</li> </ul>	US\$500 US\$790 US\$350  US\$120 US\$500	US\$150 No data No data  US\$0 US\$0	US\$0–35 No data No data  US\$0 US\$0
Exploit kit: <ul style="list-style-type: none"> <li>Eleonore Browser Exploit Kit</li> <li>Phoenix Exploit Kit</li> <li>eCore Exploit Pack</li> </ul>	US\$700 US\$600 US\$1,000	No data US\$250 No data	No data US\$0 No data
Crypter: <ul style="list-style-type: none"> <li>Basic static</li> <li>Static with stub and add-ons</li> <li>Polymorphic</li> </ul>	US\$10–30  US\$30–80 US\$100	US\$4–10  US\$15–25 US\$80	No data  US\$10–30 US\$65

Trend Micro | Russian Underground Revisited

<http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-revisited.pdf>



# Underground market prices

Russian Cybercriminal Underground Service Offerings			
Service	2011 Price	2012 Price	2013 Price
Dedicated-/Bulletproof-server hosting <ul style="list-style-type: none"> <li>• Low-end</li> <li>• High-end</li> <li>• Virtual private server (VPS)</li> </ul>	US\$160 US\$450 US\$70	US\$100 US\$160 US\$40	US\$50 US\$190 US\$12+
Proxy-server hosting (per day): <ul style="list-style-type: none"> <li>• HTTP/S</li> <li>• SOCKS</li> </ul>	US\$2 US\$2	US\$1 US\$2	US\$1 US\$2
Traffic-to-download conversion (PPI per 1,000 installations): <ul style="list-style-type: none"> <li>• Australia traffic</li> <li>• U.K. traffic</li> <li>• U.S. traffic</li> <li>• Europe traffic</li> <li>• Mixed global traffic</li> <li>• Russia traffic</li> </ul>	US\$300–500 US\$220–300 US\$100–150 US\$90–250 US\$12–15 US\$100–500	US\$200–500 No data US\$100–250 US\$75–90 US\$10–17 US\$100–190	US\$120–600 US\$150–400 US\$120–200 US\$50–110 US\$10–12 US\$140–400

Trend Micro | Russian Underground Revisited

<http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-revisited.pdf>

# Underground market prices

Russian Cybercriminal Underground Service Offerings			
Service	2011 Price	2012 Price	2013 Price
DDoS attack: <ul style="list-style-type: none"> <li>• Lasts 1 hour</li> <li>• Lasts 24 hours</li> </ul>	US\$4–10 US\$30–70	US\$2–25 US\$15–60	US\$2–60 US\$13–200
Spamming (per 10,000 messages): <ul style="list-style-type: none"> <li>• Generic (uses a public database)</li> <li>• External-email-database-based</li> <li>• SMS</li> <li>• ICQ</li> <li>• Skype</li> </ul>	US\$13  US\$17 US\$600 US\$55 No data	US\$8  US\$14 US\$300 US\$15 US\$110	US\$4–5  US\$13 US\$100 US\$4–9 US\$86
Flooding: <ul style="list-style-type: none"> <li>• Email (per 10,000 messages)</li> <li>• Landline phone</li> <li>• SMS (per 1,000 text messages)</li> </ul>	US\$30 US\$32  US\$15	US\$3 US\$23  US\$10	US\$2 US\$25  US\$8

Trend Micro | Russian Underground Revisited

<http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-revisited.pdf>

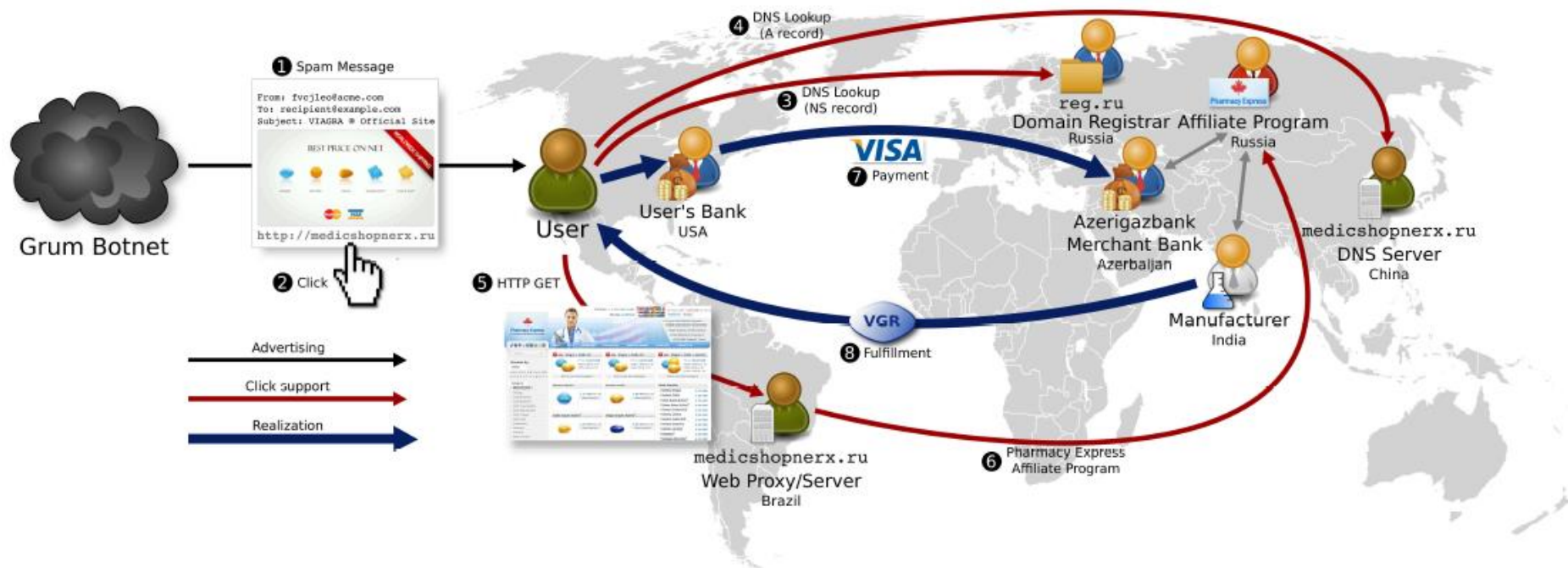
# Underground market prices

Russian Cybercriminal Underground Service Offerings			
Service	2011 Price	2012 Price	2013 Price
Malware checking against security software:			
• Daily checking	US\$50	US\$30	US\$30
• Automatic reuploading in case a piece of malware is being detected by known anti-malware solutions	US\$50	US\$30	US\$30
• Checking against malicious URL blacklists	US\$50	US\$30	US\$30
Hacking:			
• Facebook account	US\$200	US\$160	US\$100
• VK account	US\$120–140	US\$100	US\$76
• Odnoklassniki account	US\$94	US\$90	US\$94
• Twitter account	US\$167	US\$40	No data
• Gmail account	US\$117	US\$120	US\$100
• Mail.ru account	US\$74	US\$70	US\$50
• Yandex.ru account	US\$74	US\$70	US\$50
• Hotmail account	US\$107	US\$100	US\$100

Trend Micro | Russian Underground Revisited

<http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-revisited.pdf>

# Example: Spam



taking down such an international organization is a challenge!

**MALWARE**

# Malware

- malware = malicious software
  - a.k.a. malicious code or malcode
- any code that can be added to a software system in order to intentionally cause harm or subvert the intended function of the system
- generic term that encompasses viruses, worms, Trojans, and other intrusive code



# Recent trends in malware development

- mass malware development is driven by cybercrime
- malware for smart devices proliferate
- malware is extensively used in state sponsored targeted attacks (cyberwar?)



# Mass malware and cybercrime

- malware infected computers represent value for criminals
  - theft of personal information and account credentials (e.g., passwords)
    - » stolen information can be used directly or sold on underground markets
  - man-in-the-middle attacks
    - » e.g., compromised browser may alter e-banking transactions (ZeuS)
    - » e.g., compromised smart phone may intercept and redirect SMS messages containing one-time transaction authorization tokens
  - use of computing resources
    - » infected computers can be organized into botnets and used for spam, DDoS, and click fraud
    - » infected computers can be used for bitcoin mining
  - ransom
    - » hard disk of infected computer can be encrypted and decryption key can be revealed only after some payment
- malware itself can be monetized
  - malware can be sold on underground markets



# Malware for smart devices

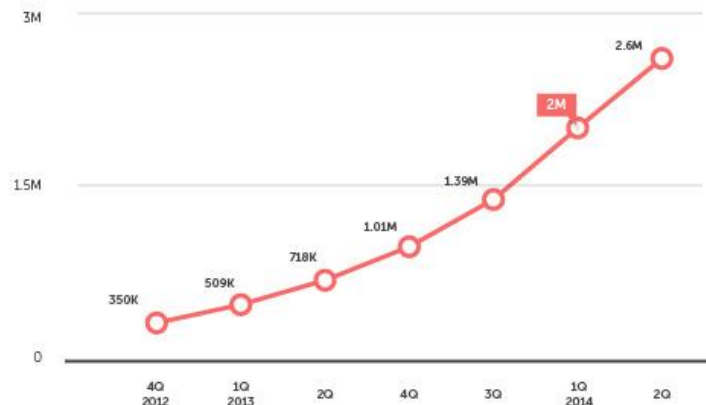
- for criminals, there's not much difference between a PC and a smart phone as a potential target
    - smart phones have considerable computing power
    - they are always on and connected to the network
    - they run all sorts of applications originating from different sources
      - » users use them for sensitive tasks too
      - » new (potentially malicious) applications can be installed on them
    - they store or have access to large amount of personal information
    - number of smart phones is large enough → it is worth attacking them
- compromising smart phones represents new revenue sources for attackers
- consequently, number of malware for smart phones has been increasing exponentially in the last few years

# Mobile malware history and growth rate

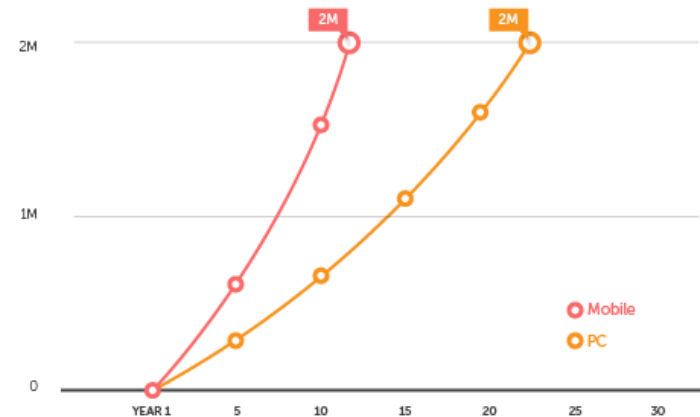


<http://www.sophos.com/en-us/threat-center/mobile-security-threat-report.aspx>

Mobile Malware and High-Risk App Total Count



PC and Mobile Malware Growth Rate

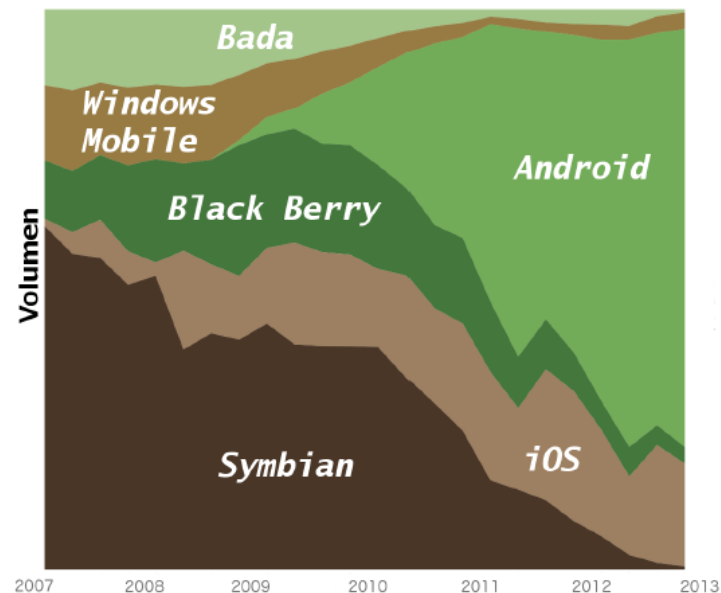


<http://www.trendmicro.com/vinfo/us/security/news/mobile-safety/the-mobile-landscape-roundup-1h-2014>

# Market share vs. malware volume

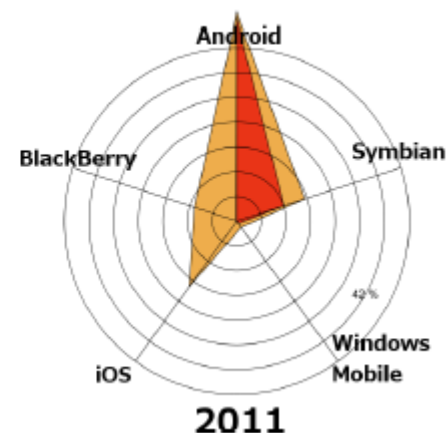
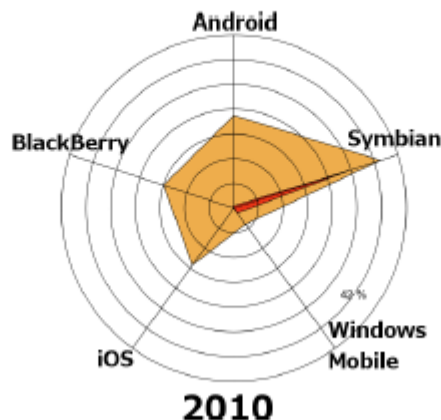
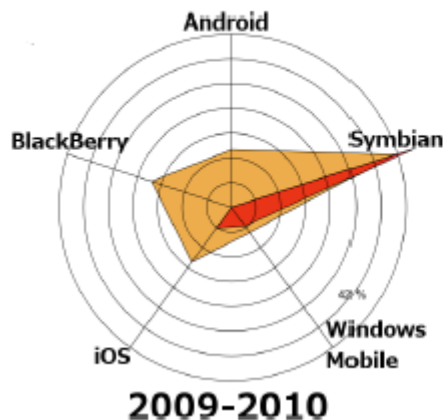
## Android vs. iOS

- Apple has a more rigorous app review process
- iOS apps are signed, developer certificates are issued only after obtaining a verified Apple credential
- Google relies more on platform protection mechanisms (permissions and sandboxing)
- Android apps are signed, but developer certificate can be self-signed
- **Android apps are also distributed via alternative app markets**



■ Malware  
■ Market Share

## Malware and Market Share Correlation



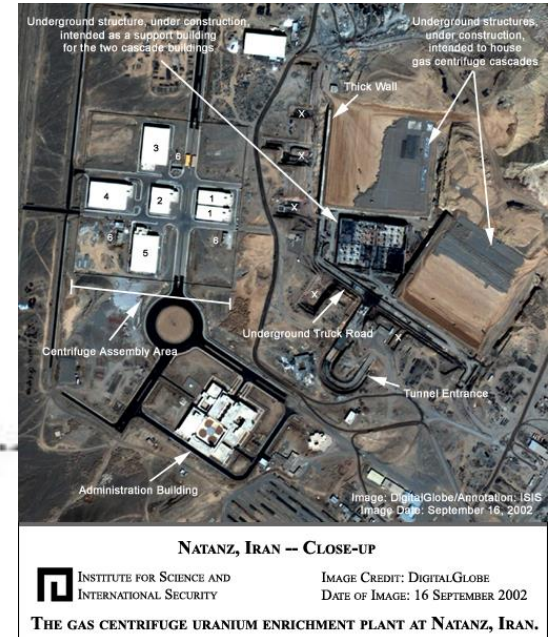
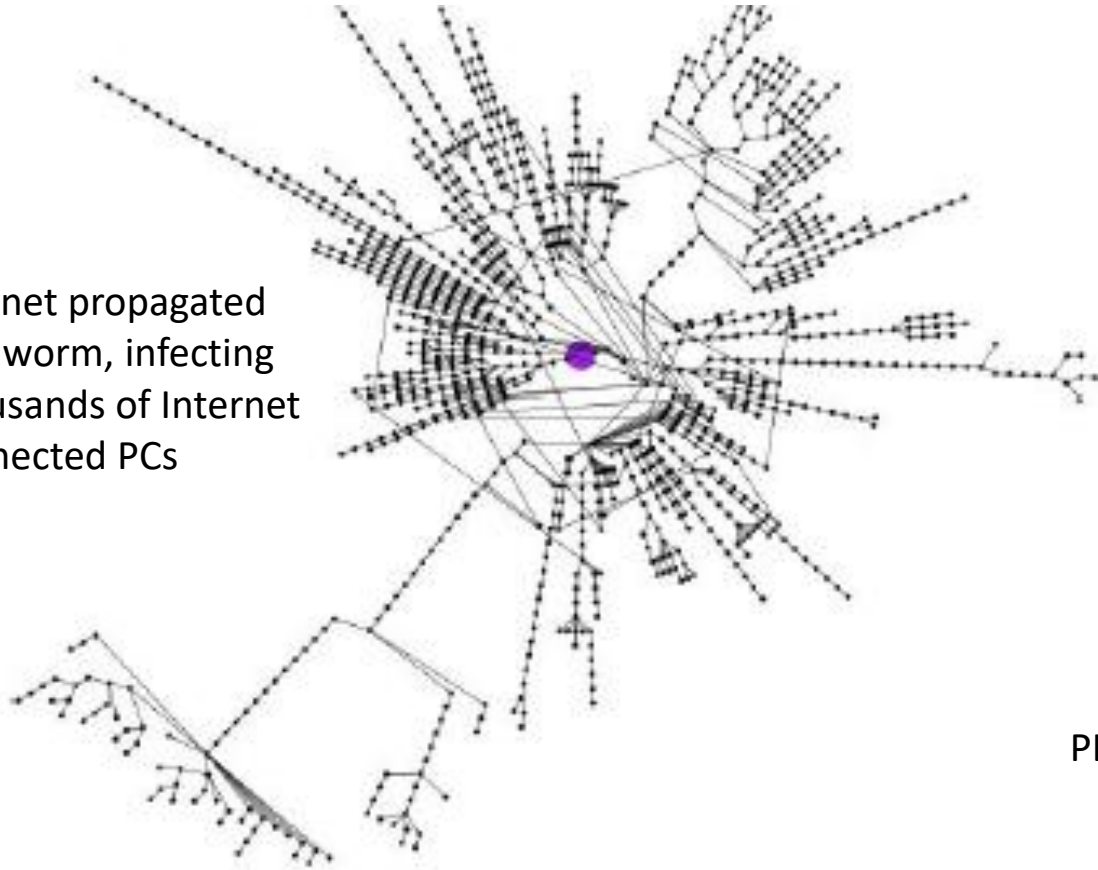
G. Suarez-Tangil, J. E. Tapiador, P. Peris-Lopez, A. Ribagorda, Evolution, Detection and Analysis of Malware for Smart Devices, IEEE Communications Surveys and Tutorials, 2014.

# Malware for targeted attacks

- malware can be used in attacks targeting a given organization or set of individuals with the objective of
  - espionage
  - sabotage
- often, infecting the computers of the target by some malware is the easiest or cheapest way to reach the above objectives
- attackers behind such attacks are often military or state intelligence organizations (a.k.a. Advanced Persistent Threats)

# Example: Stuxnet (June 2010)

Stuxnet propagated as a worm, infecting thousands of Internet connected PCs



once inside the target environment, it reprogrammed PLCs and caused physical damage

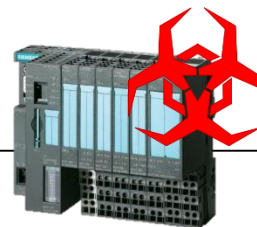
# Example: Stuxnet (June 2010)

- “the Most Menacing Malware in History” (Kim Zetter, Wired)
- targeted the Natanz nuclear enrichment plant in Iran
- used multiple zero-day exploits
- possibly created by Western nation states

PC running WinCC PLC management software

PLC controlling the uranium centrifuges

uranium centrifuges



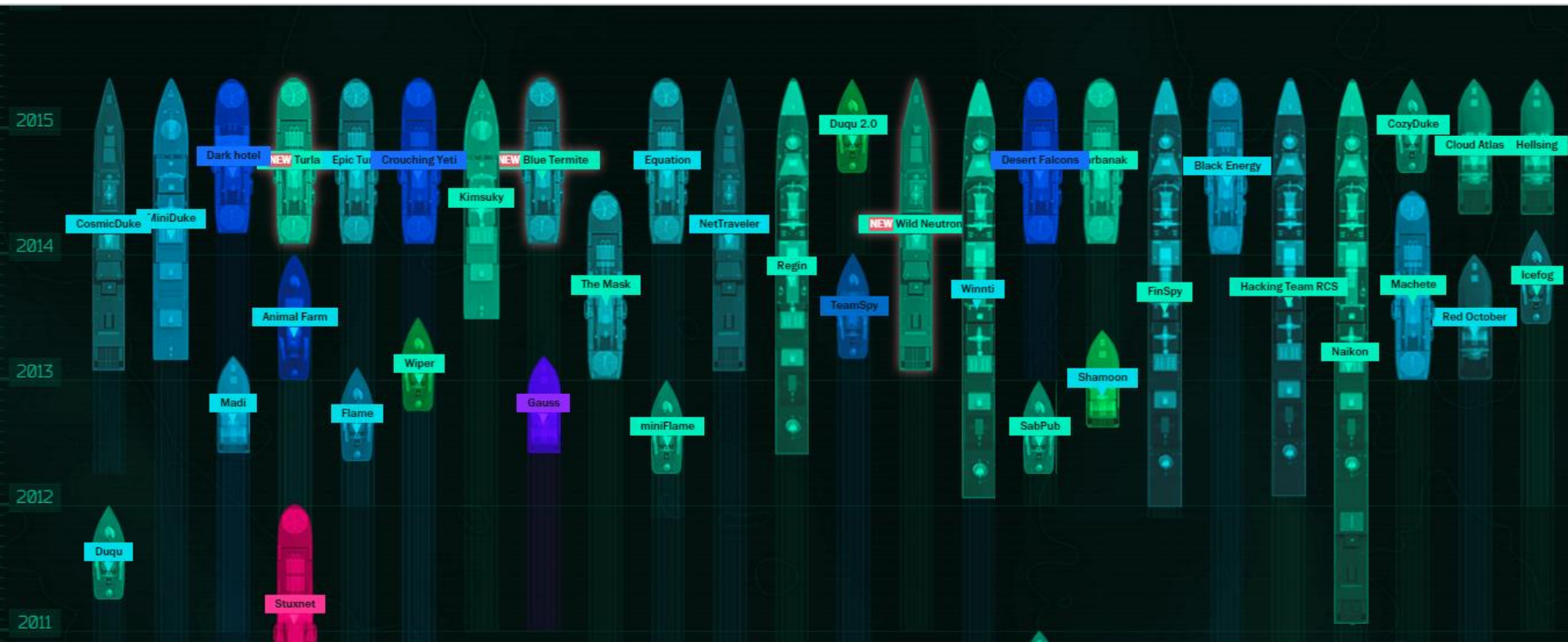
Stuxnet infected PCs, and took over the communication between the PC and the PLC

then modified the PLC program

modified program destroyed centrifuges



# Other examples



<https://apt.securelist.com/>

# Advanced Persistent Threats

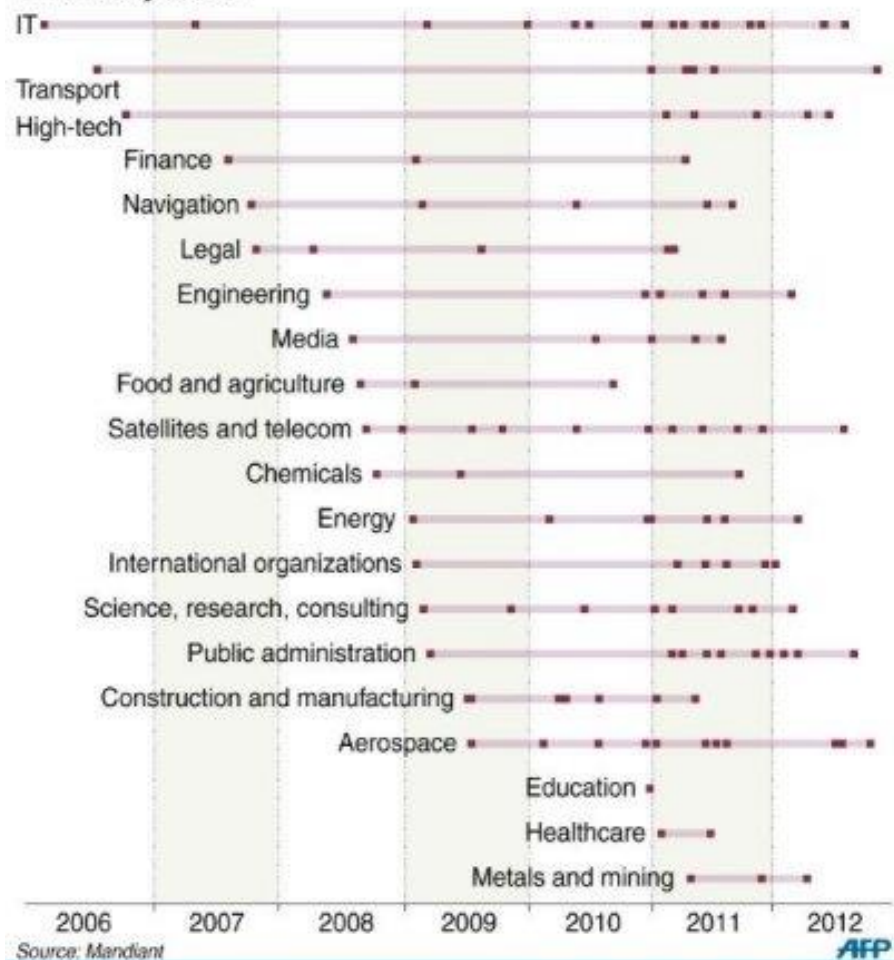
- APT1 (PLA Unit 61398)
  - nearly 150 victims over 7 years
  - maintained access to victim networks for an average of 356 days
  - size of its infrastructure implies a large organization with at least dozens, but potentially hundreds of human operators



## Hacked by APT1

Industries that have been targeted by the China-based espionage group APT1, according to US security firm Mandiant

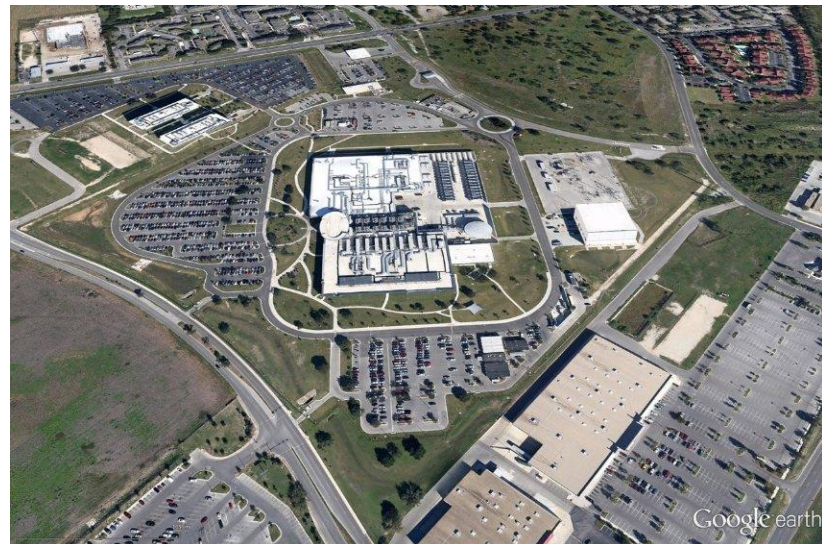
### Timeline by sector





# Advanced Persistent Threats

- Office of Tailored Access Operations (TAO)
  - cyber-warfare intelligence-gathering unit of the NSA
  - identifies, monitors, infiltrates, and gathers intelligence on computer systems being used by entities foreign to the United States (computer network exploitation)
  - has tools for breaking into commonly used hardware, including routers, switches, and firewalls from multiple product vendor lines



REMOTE CONTROL SYSTEM

GALILEO

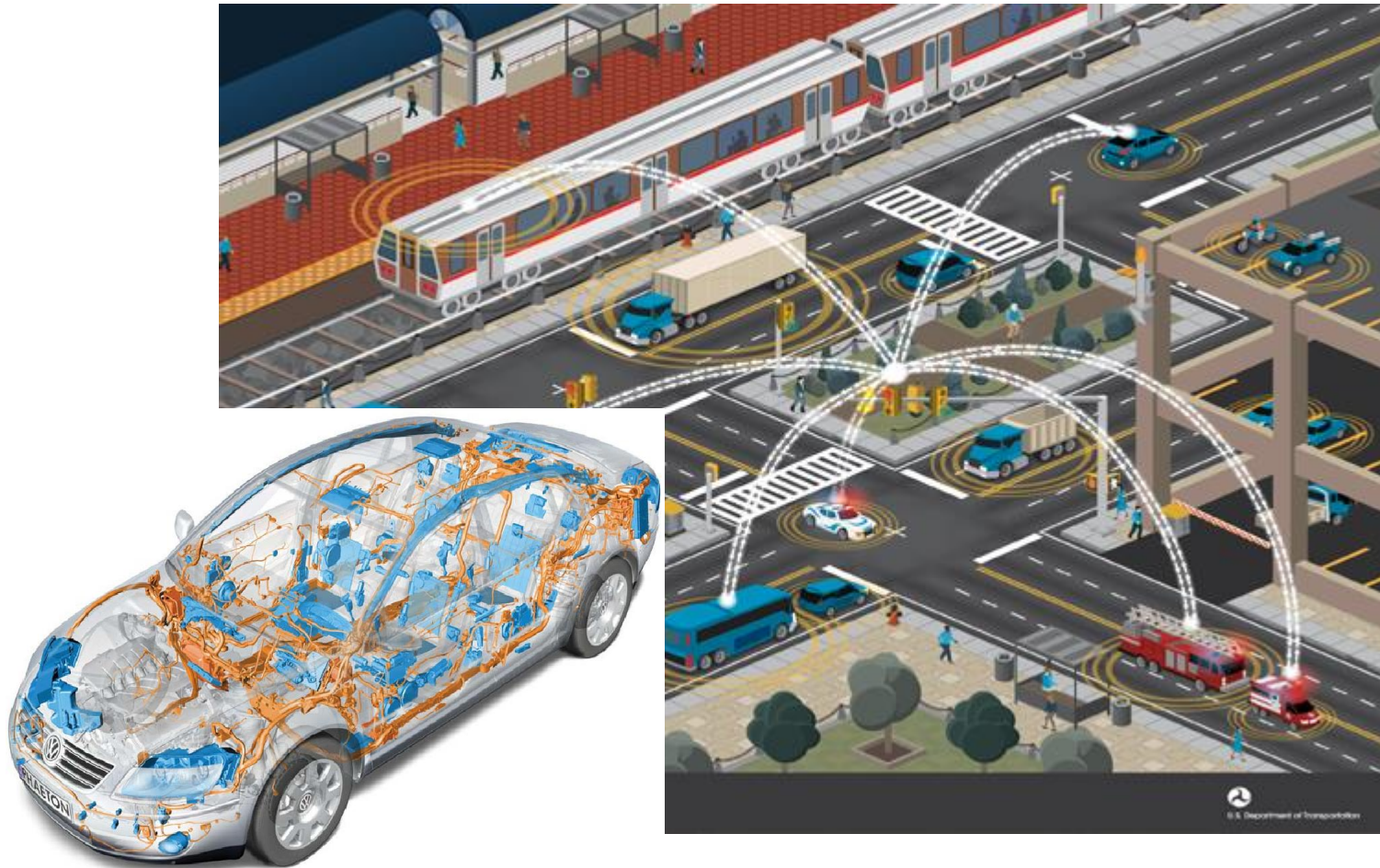
[www.comsoc.org/blog](http://www.comsoc.org/blog)

# Smart homes

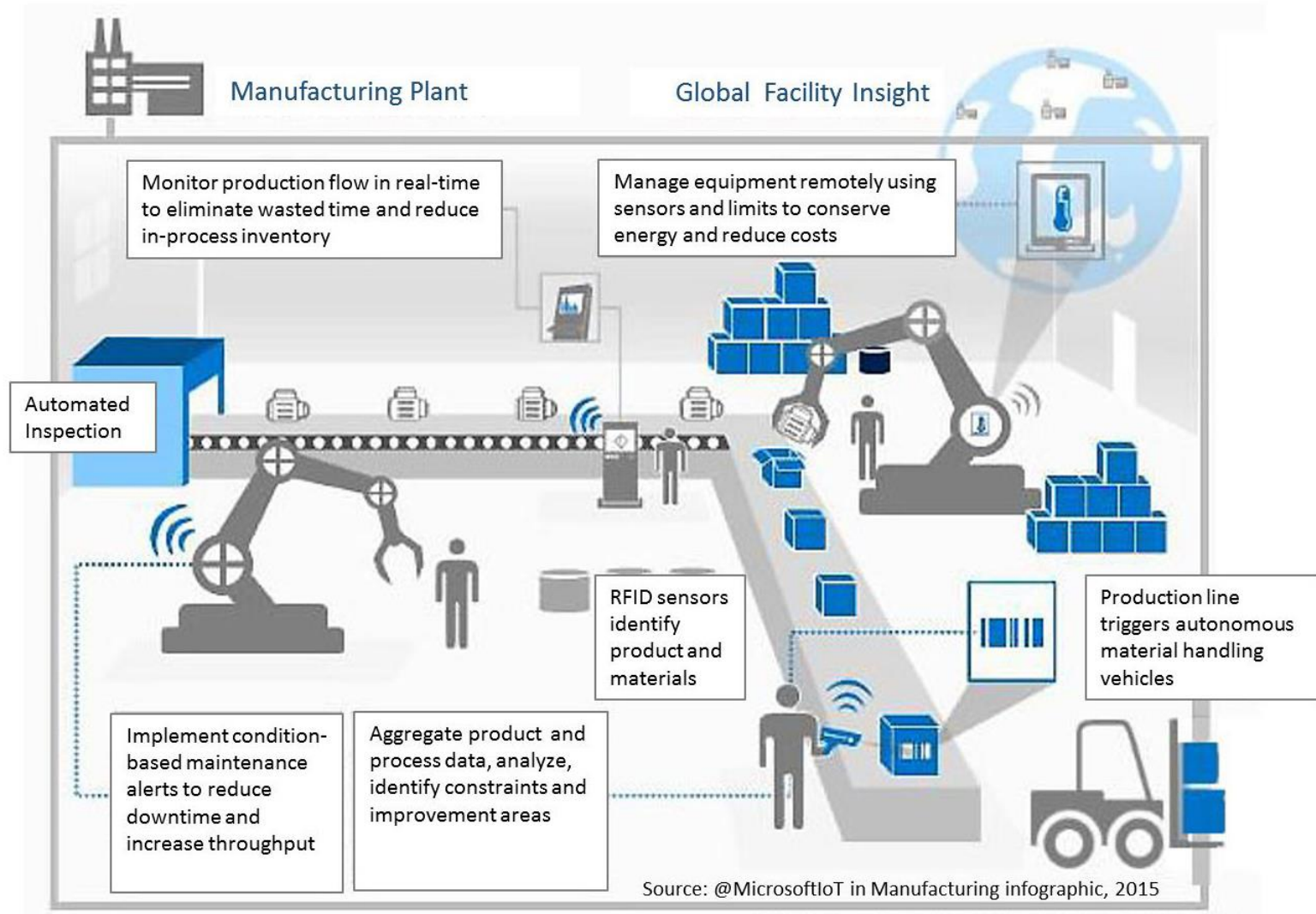




# Intelligent Transport Systems



# Smart factories (aka Industry 4.0)



# How about security?

SECURITY

## No surprise, IoT devices are insecure

By

— Hacking a living room: Kaspersky Lab researcher finds



H  
in  
Fir  
by S

Repo

David Shep

ENTREPRENEURS

8/03/2013 @ 8:08PM | 15,132 views

### Hacking Insulin Pumps And Other Medical Devices From Black Hat

+ Comment Now + Follow Comments

PODCASTS

king



(Photo: Detroit News, file)

### Traffic Monitoring Tech Vulnerable To Hacking

POSTED BY: PAUL MAY 1, 2014 11:36 COMMENTS OFF

re

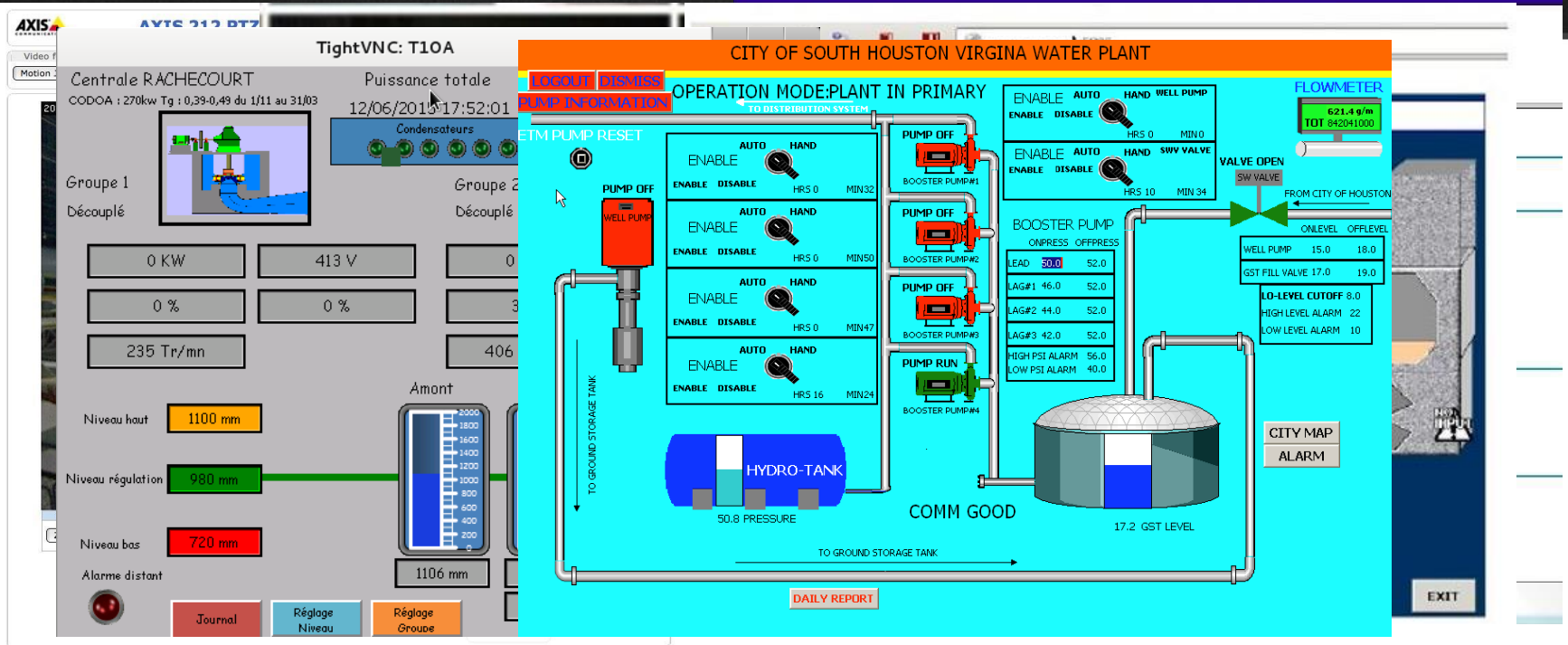
by

Connected cars aren't the only **transportation** innovation that's coming down the pike (pun intended). As **we've noted before**: smart roads and smart **infrastructure** promise even more transformative changes than – say – having Siri read your text messages to you through your stereo system.



# How about security?

The image shows the top portion of the Shodan website. At the top, there is a navigation bar with links for 'Shodan', 'Developers', 'Book', and 'View All...'. Below this is a dark header containing the Shodan logo (three red circles), a search bar with a magnifying glass icon, and links for 'Explore', 'Enterprise Access', and 'Contact Us'. On the right side of the header are links for 'New to Shodan?' and 'Login or Register'. The main hero section features a large, stylized globe composed of a wireframe grid. Overlaid on the globe is the text 'The search engine for the Internet of Things' in a large, bold, white font. Below this, a smaller line of text states 'Shodan is the world's first search engine for Internet-connected devices.' At the bottom of the hero section, there are two buttons: 'Create a Free Account' (red) and 'Getting Started' (blue). The background of the hero section is dark with some faint, glowing red and white patterns.





## Internet of Things

```
graph TD; A[Internet of Things] --> B[now easily searchable and accessible remotely]; A --> C[cheap (in every sense) computers easy to compromise];
```

now easily searchable and  
accessible remotely

cheap (in every sense)  
computers easy to compromise

# IoT devices became the weakest link



# Default passwords

[Home](#) | [Add Password](#) | [About](#)

## RouterPasswords.com

*The Roadmap to Modern IT Operations*  
Do you have what you need for your business' Digital Transformation?

FREE DOWNLOAD

pagerduty

Welcome to the internet's largest and most updated default router passwords database.

Select Router Manufacturer:

CISCO

Find Password

Manufacturer	Model	Protocol	Username	Password
CISCO	CACHE ENGINE	CONSOLE	admin	diamond
CISCO	CONFIGMAKER		cmaker	cmaker
CISCO	CNR Rev. ALL	CNR GUI	admin	changeme
CISCO	NETRANGER/SECURE IDS	MULTI	netrangr	attack
CISCO	BBSM Rev. 5.0 AND 5.1	TELNET OR NAMED PIPES	bbsd-client	changeme2
CISCO	BBSD MSDE CLIENT Rev. 5.0 AND 5.1	TELNET OR NAMED PIPES	bbsd-client	NULL
CISCO	BBSM ADMINISTRATOR Rev. 5.0 AND 5.1	MULTI	Administrator	changeme
CISCO	NETRANGER/SECURE IDS Rev. 3.0(5)/S17	MULTI	root	attack
CISCO	BBSM MSDE ADMINISTRATOR Rev. 5.0 AND 5.1	IP AND NAMED PIPES	sa	(none)
CISCO	CATALYST 4000/5000/6000 Rev. ALL	SNMP	(none)	public/private/secret
CISCO	PIX FIREWALL	TELNET	(none)	cisco
CISCO	VPN CONCENTRATOR 3000 SERIES Rev. 3	MULTI	admin	admin
CISCO	CONTENT ENGINE	TELNET	admin	default
CISCO	AP1200 Rev. IOS	MULTI	Cisco	Cisco

# Unpatched vulnerabilities



## 12-Year-Old SSH Bug Exposes More than 2 Million IoT Devices

📅 Thursday, October 13, 2016 👤 Mohit Kumar

New research [[PDF](#)] published by the content delivery network provider Akamai Technologies shows how unknown threat actors are using a 12-year-old vulnerability in OpenSSH to secretly gain control of millions of connected devices.

"New devices are being shipped from the factory not only with this vulnerability exposed but also without any effective way to fix it. We've been hearing for years that it was theoretically possible for IoT devices to attack. That, unfortunately, has now become the reality."

# Factory made backdoors

Saturday, September 26, 2015

## How I hacked my IP camera, and found this backdoor account



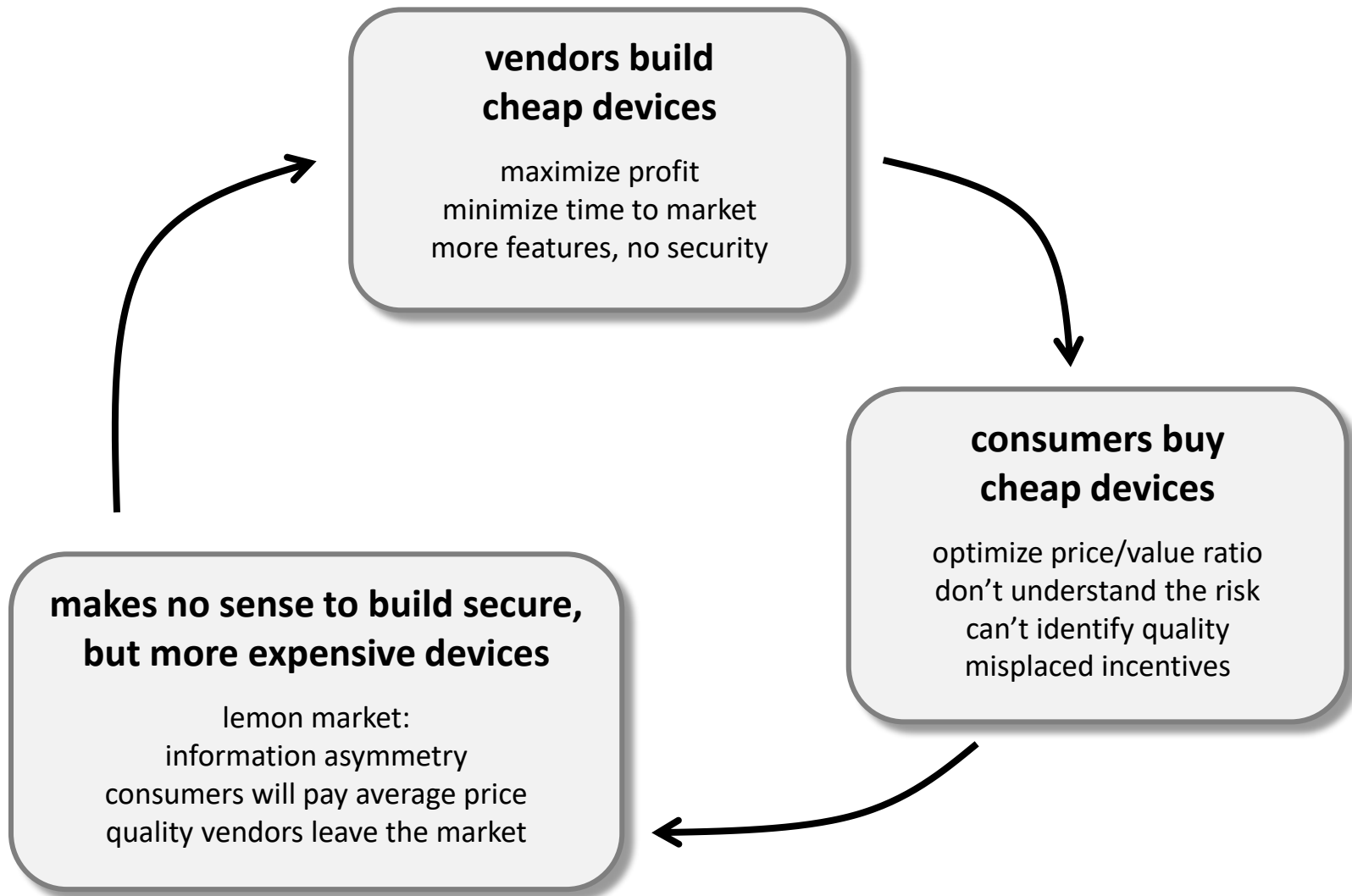
It is time to recap what we have. There is an undocumented telnet port on the IP camera, which can be accessed by default with root:123456, there is no GUI to change this password, and changing it via console, it only lasts until the next reboot. I think it is safe to tell this a backdoor.

With this console access we can access the password for the FTP server, for the SMTP server (for alerts), the WiFi password (although we probably already have it), access the regular admin interface for the camera, or just modify the camera as we want. In most deployments, luckily this telnet port is behind NAT or firewall, so not accessible from the Internet. But there are always exceptions. Luckily, UPNP does not configure the Telnet port to be open to the Internet, only the camera HTTP port 81. You know, the one protected with the 4 character numeric password by default.

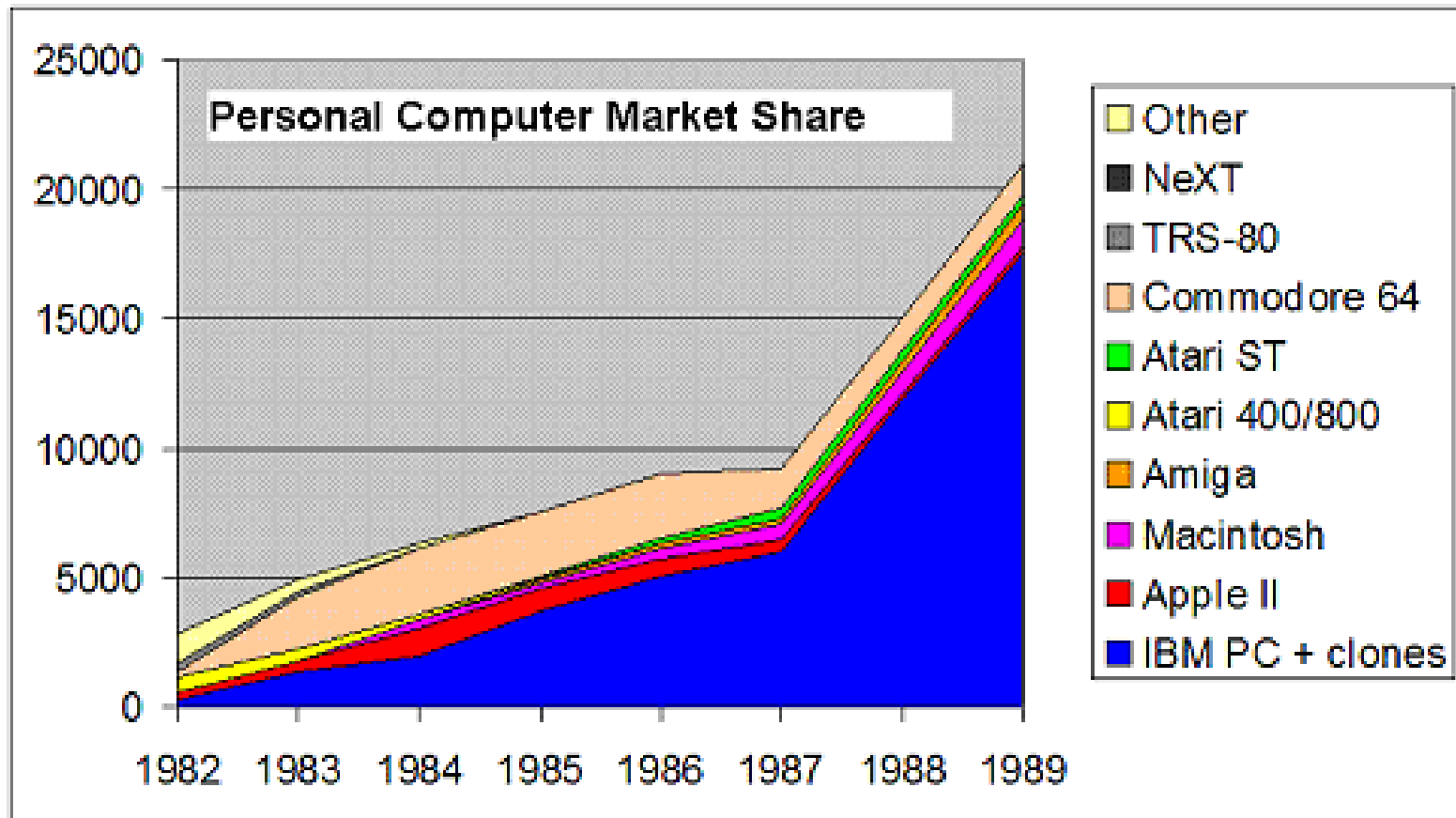
Posted by Z at 2:02:00 PM



# Security economics



# Have you seen this before?







**“History is just new people making old mistakes.”**

— Sigmund Freud

# Consequences can be dramatic...



**NETWORKWORLD**  
FROM IDG



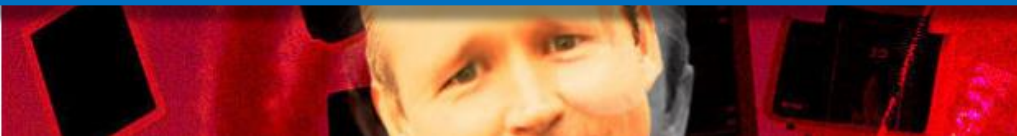
By Tim Greene | [Follow](#)

Network World | Sep 23, 2016 10:53 AM PT

## Largest DDoS attack ever delivered by botnet of hijacked IoT devices

RELATED

The delivery network has dropped protection for the [Krebs on Security](#) blog written by Brian Krebs after an attack delivering **665Gbps** of traffic overwhelmed his site Tuesday. The size of the attack was nearly double that of any Akamai had seen before.



Armies of hacked IoT devices launch unprecedented DDoS attacks

# Consequences can be dramatic...

**PCWorld**  
FROM IDG

NEWS REVIEWS HOW-TO VIDEO B

## Major DDoS attack knocks Spotify, PayPal, and more

The sound of silence.

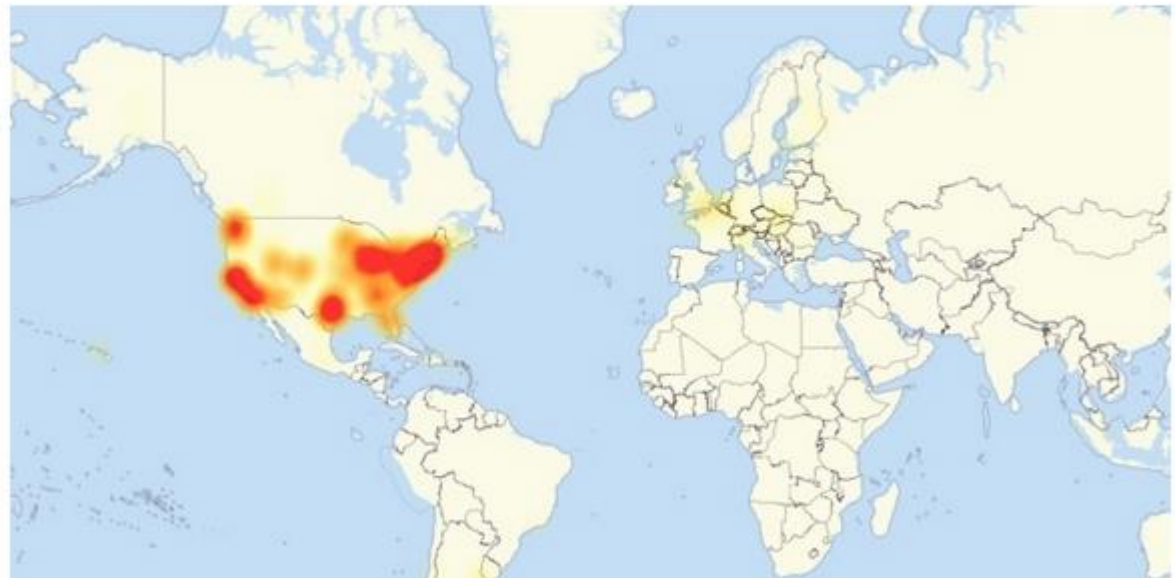


Brad Chacos | [@BradChacos](#)  
Senior Editor, PCWorld

Oct 21,

## An IoT botnet is partly behind Friday's massive DDoS attack

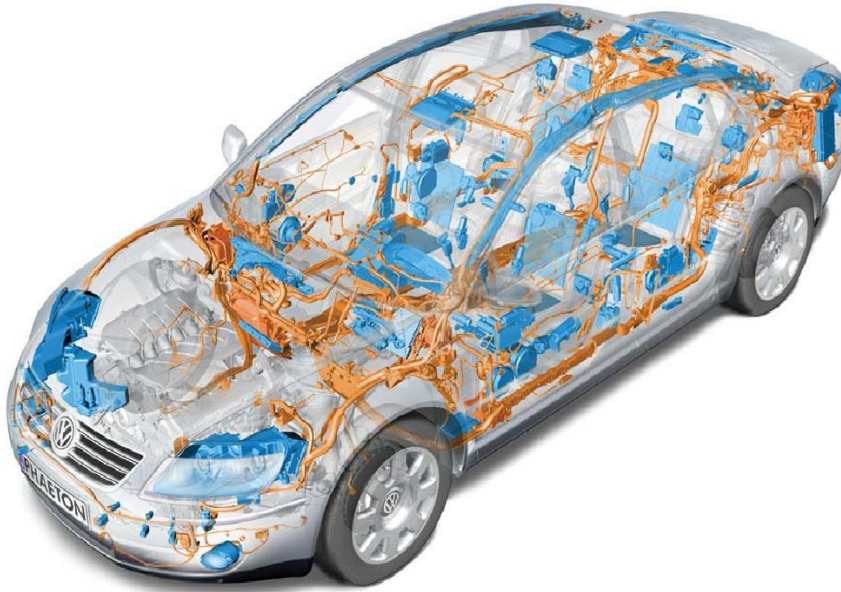
DVRs and other devices compromised with the Mirai malware are being the attack.



Michael Kan  
IDG News Service

Oct 21, 2016 4:21 PM

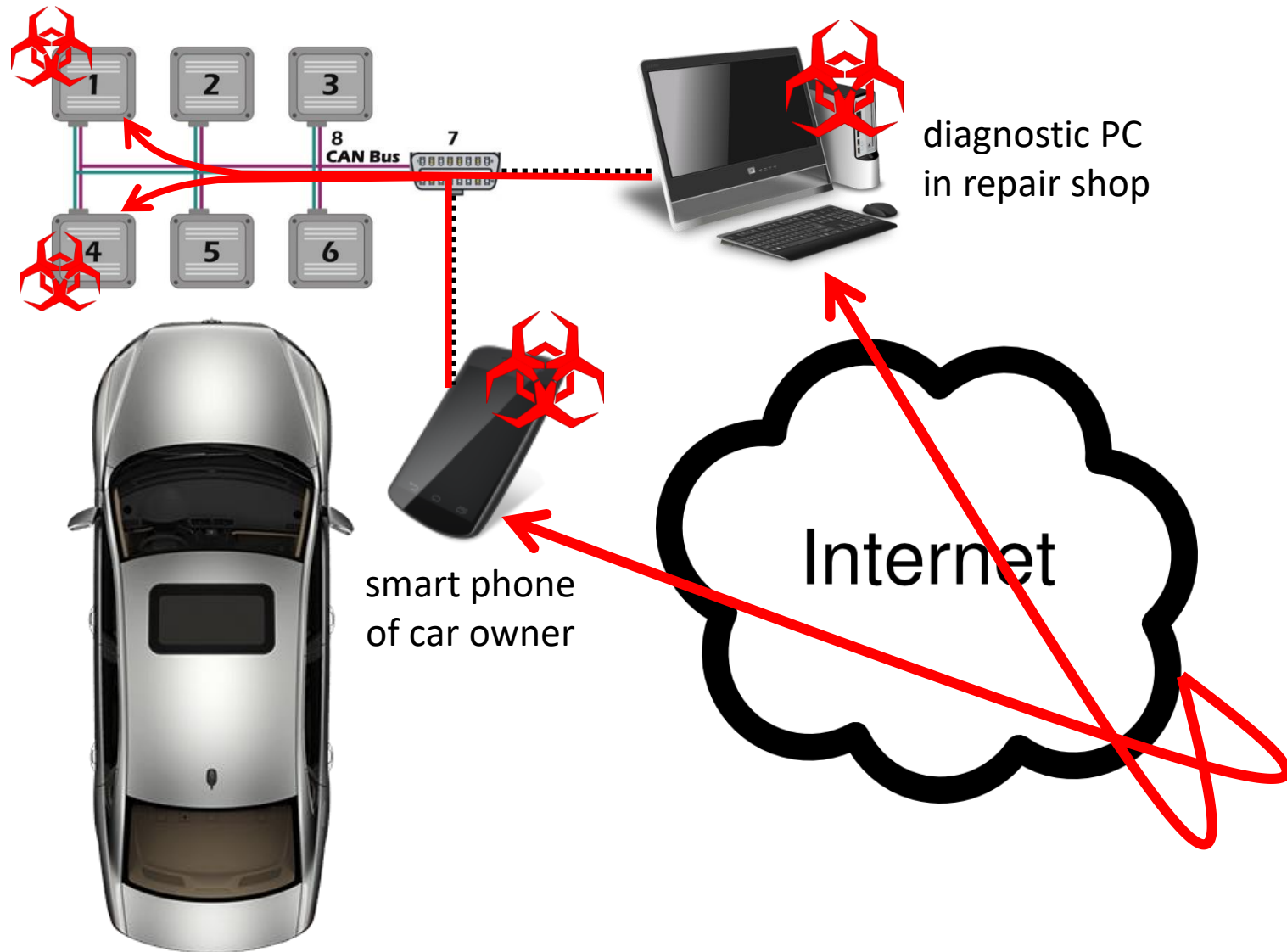
# IT security of vehicles



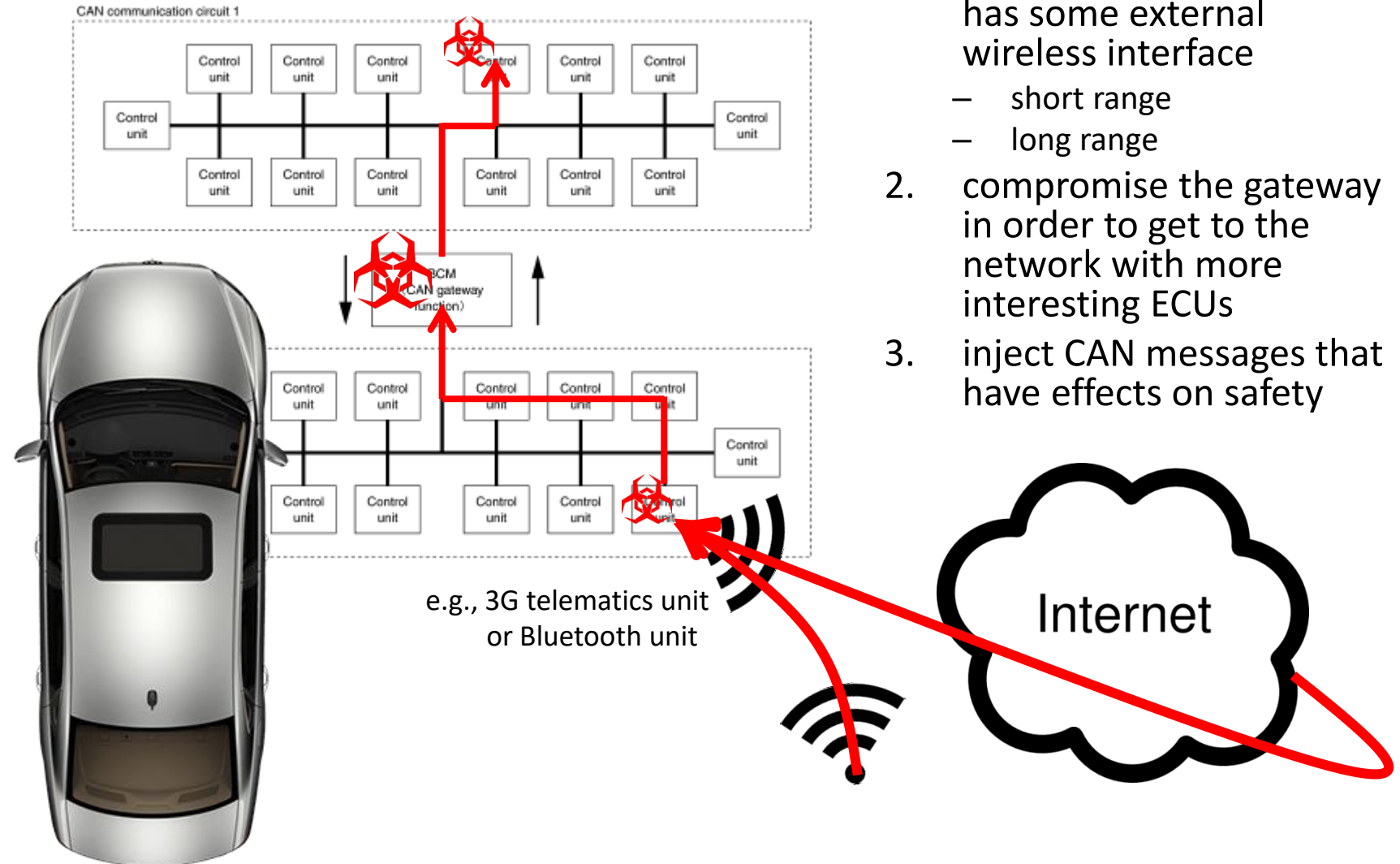
"Your car is no longer a mechanical device with some computers inside; it's a computer with four wheels and an engine."

-- Bruce Schneier, security expert

# Cyber attacks on vehicles – part 1



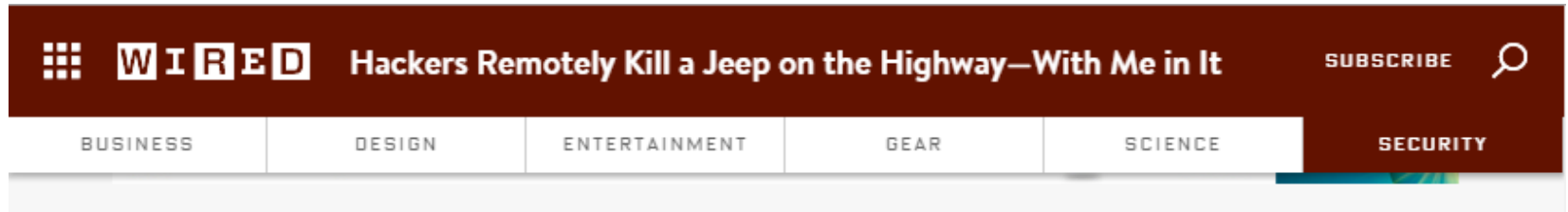
# Cyber attacks on vehicles – part 2



1. compromise an ECU that has some external wireless interface
  - short range
  - long range
2. compromise the gateway in order to get to the network with more interesting ECUs
3. inject CAN messages that have effects on safety



# Cyber attacks on vehicles – part 2




ANDY GREENBERG SECURITY 07.21.15 6:00 AM

## HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT





<https://www.youtube.com/watch?v=MK0SrxBC1xs>

# Conclusions




MORE ACM AWARDS






Search



A.M. TURING AWARD WINNERS BY...

ALPHABETICAL LISTING	YEAR OF THE AWARD	RESEARCH SUBJECT
----------------------	-------------------	------------------




## ADI SHAMIR


Israel – 2002

**CITATION**


Together with Leonard M. Adleman and Ronald Rivest, for their ingenious contribution to making public-key cryptography useful in practice.




SHORT ANNOTATED BIBLIOGRAPHY




ACM DL AUTHOR PROFILE



ACM TURING AWARD LECTURE VIDEO



RESEARCH SUBJECTS



ADDITIONAL MATERIALS

Internet (in)security | 64



# Conclusions



1. Cybersecurity is terrible, and will get worse.

2. The Internet of Things will be a security disaster.

...

**Adi Shamir makes 15 predictions for the next 15 years!**

Published on February 29, 2016

# The good news is ...

JAN 2, 2016 @ 09:06 AM 148,016 VIEWS

Forbes

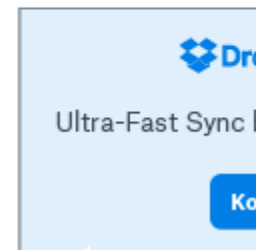
## One Million Cybersecurity Job Openings In 2016



**Steve Morgan**, CONTRIBUTOR

*I write about the business of cybersecurity.* [FULL BIO](#) ✓

Opinions expressed by Forbes Contributors are their own.



If you are thinking about a career change in 2016, then you might want to have a look at the burgeoning cybersecurity market which is expected to grow from \$75 billion in 2015 to \$170 billion by 2020.

A knack for cat and mouse play may indicate that you have an aptitude for cybersecurity. It is a field where the good guys — cybersecurity professionals — are pitted against the bad guys — cybercriminals a.k.a. hackers. Assuming you'd want to be a good guy — a career can mean a six-figure salary, job security, and the potential for upward mobility.

More than 209,000 cybersecurity jobs in the U.S. are unfilled, and postings are up 74% over the past five years, according to a 2015 analysis of numbers from the Bureau of Labor Statistics by Peninsula Press, a project of the Stanford University Journalism Program.