Session 01 Overview of Data and Network Security

CS7349

Spring 2024

World Changers Shaped Here

SMU®

© Shaibal Chakrabarty

Learning Objectives

- **Understand** the basics of **security**
- Ability to discuss **security and privacy issues**
- Understand fundamental security **mechanisms**
- Understand **how** fundamental security **mechanisms** are used to provide security
- Develop **security analysis and team skills** through the completion of a group project
- Develop **oral and written communication skills** via class presentations

Expectations

- Attend and **come prepared** to participate in classes
- **Perform** all assignments for CS7349 in a timely manner
- Produce a **publishable** technical paper as a team project
- Submissions should be semi-professional at the minimum

Assignment weighting

Assignment	Weighting
Homeworks (2)	20%
Case Study	10%
Exams (2)	30%
Weekly Participation+Quizzes	10%
Semester Paper	30%

- Term project will be a collaborative effort with a maximum of 3 members. The team will present the paper to the class prior to submission. Publishable papers are expected to suggest a new proposal, and include a basic implementation

Honor Code

- When you signed your letter of intent to enroll in the program, you initialed the following statement:
- “I have read and agree to abide by the SMU Honor Code available online at: http://www.smu.edu/StudentAffairs/StudentLife/StudentHandbook/HonorCode”
- Please know that the Honor Code is taken very seriously.

Honor Code Violations*

- Academic Sabotage
- Cheating
- Fabrication
- Facilitating academic dishonesty
- Plagiarism

***http://www.smu.edu/StudentAffairs/StudentLife/StudentHandbook/HonorCode**

Plagiarism

- Here is an example of plagiarism:

A regression is a statistical analysis assessing the association between two variables. It is used to find the relationship between two variables.

- The following is NOT plagiarism:

“A regression is a statistical analysis assessing the association between two variables. It is used to find the relationship between two variables.”[1]

- The difference is in the punctuation and the attribution.
- Note that one can self-plagiarize. If you are using something that you wrote (e.g. a blog or a previously published article), please reference yourself.

[1] **(https://www.easycalculation.com/statistics/learn-regression.php).**

Consequences

- Plagiarism, sabotage, fabrication, and cheating carry high penalties.
- Instructors may choose to fail the student on the assignment, give a 0 for the assignment, fail the student for the course, and/or bring the student before the Honor Council.
- Honor Council violations (if convicted) go on the student’s transcript.

Assignment Expectations

- All assignments: Homeworks, Case Study, Exams are take-home, open book and collaborative
  - Submissions are INDIVIDUAL and should not be identical/similar
- References and collaborators should be cited (extra credit)
- Homeworks and Case Study: A well-formatted report, clearly labeling the responses, with references and figures
- Exams: Multiple-choice will require explanation for each choice. Includes all the above expectations

Team Projects/Paper

- Choose a security topic of common interest
- Within topic, identify problem to be addressed (no review projects, only problem solving projects - review is a natural part of your problem solution and is contained in the final paper)
- Confirm problem with professor
- Identify your team and team leader
- Be ready to make an 8-10 min presentation of your paper at semester end.

Project Timeline (For 9 page paper)

- Jan: First project draft 1 page, basically your Introduction section, plus title, authors and abstract, some references
- Feb: Interim draft 3 pages, basically your intro and related work, plus basic description of your solution
- Mar: Draft 6 pages. Detailed solution, analysis, references
- Apr: Final paper 9 pages. Submit, with presentation

A LaTex template and example paper will be provided

Project – 1st deliverable

- Team projects (3 per team)
- Choose topic (from topic list or your own)*
- Within topic, identify problem to be addressed (no survey projects, only problem solving projects - survey is a part of your problem solution and is contained in the final paper)
- Confirm problem with professor

Project Abstract and Intro

- **Abstract** structure (150 word limit for 9 pages)
  - start with statement of what is presented
  - motivate the problem
  - discuss details of what is done at a high level
  - state the main conclusions
- **Introduction** basic structure (the rest of page 1):
  - motivate the problem further
  - state the problem in detail
  - state the basic work done/approach taken
  - State the contributions of your paper
  - state the outline for the rest of the paper
    - Conclusions are not stated in the introduction.

Project Reports

- **Use the LaTex template** provided for all of your project paper submissions.
- Your paper is expected to be publishable
  - High quality research, well written, reproducible results based on paper contents. 6 pages. No more, no less
  - https://scholar.google.com/ for references (NOT cnn.com, foxnews.com, cnbc.com; YES ietf.org, ieee.org,…itu-t)
  - https://www.overleaf.com/latex/templates/preparation-of-papers-for-ieee-sponsored-conferences-and-symposia/zfnqfzzzxghk (online template for IEEE format – get account)

Contents

- Introduction
- Chapters
- Let’s explore
- Deliverables
- Your feedback

Spring schedule

Date	Week/Unit	Learning Material	Assignment
01/17/2024	1/1	Intro to Data and Network Security	Stallings Ch 1; Quiz#1;Start project team, select project and inform instructor
Jan 22, 24	2/2	Intro to Computer Networks	Submit Quiz #2; Project team confirms problem with instructor/Homework 1 issued/Term paper checkpoint
Jan 29, 31	3/3	Symmetric Key Cryptography	Stallings Ch 2-3; Submit Quiz #3; First Project Draft (Title, authors, abstract and Intro)/
Feb 5, 7	4/4	Using Symmetric Key Ciphers	Stallings Ch 3-6; Submit Quiz#4 (ch03 and ch06); Homework #2 issued
Feb 12, 14	5/5	Randomness and Pseudorandom Numbers	Stallings Ch 7; Submit Quiz #5/Term Paper Checkpoint
Feb 19, 21	6/6	Public Key Cryptography	Stallings Ch 9-10; Submit Quiz #6/Case Study Due/
Feb 26, 28	7/7	Hash Functions/	Stallings Ch 11; Submit Quiz #7; Paper Interim Draft; Exam 1 issued
Mar 4, 6	8/8	Message Authentication Codes	Stallings Ch 12; Submit Quiz#8;
Mar 11, 13	9/9	SPRING BREAK!!!	
Mar 18, 20	03/10	Key Management and Key Distribution	Stallings Ch 14; Submit Quiz #10/Term paper checkpoint/Start on project presentation/Case Study
Mar 25, 27	04/11	User Authentication	Stallings Ch 15; Submit Quiz #11/
Apr 1, 3	12/12	Network Security	Stallings Ch 17; Submit Quiz #12; Presentation check/Exam #2
Apr 8, 10	13/13,14	Privacy, Security Ethics	
Apr 15, 17	14	Applications: AI and Quantum Computing	Submit Final Project Paper
Apr 22, 24	15	Open	Presentations of Term Project by class/
Apr 29		Wrap up and Review	
This schedule is subject to changes. All assignments are due by 11:59pm of the due date. Earlier submissions are encouraged and welcome. Do not wait till the last moment.			
You will have 2 weeks to complete most assignments.			

Book: Cryptography and Network Security by William Stallings, 8th edition

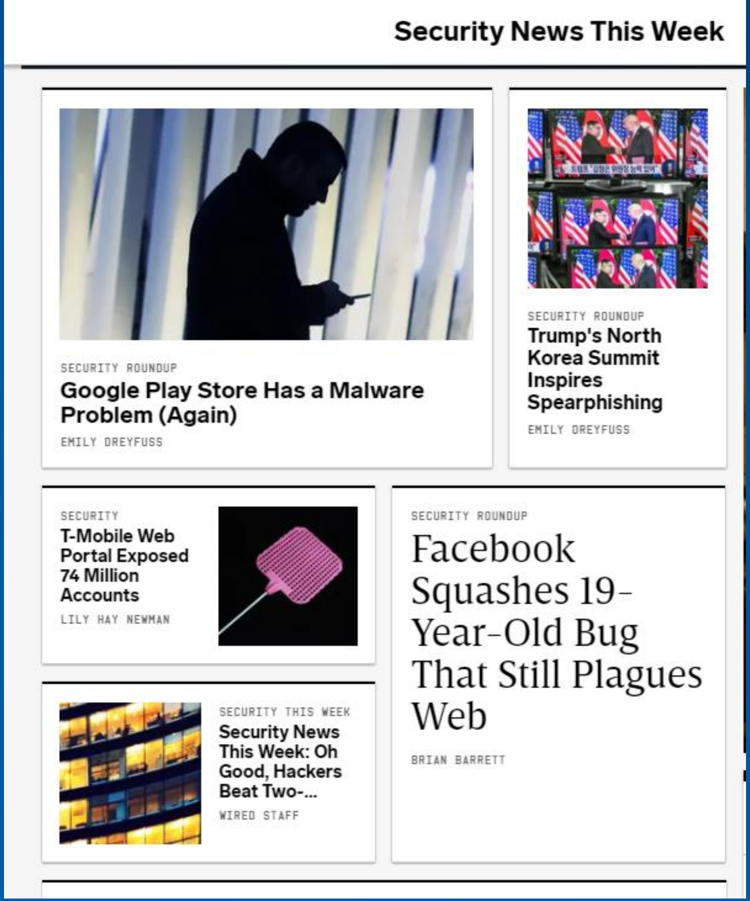
House Keeping (Example)

- Quiz 01 due at 23:59 on 02/03/21
- HW 1 is due by 02/22/2024
- Term Project is due 04/xx/2024 by 23:59
- Guest Lecture by **
  - Review Class (April)

Class Presentation – 1 presentation/class

- Any topic of your interest: Work, play
  - Can be a question/answer, wonderment, information
  - **Security related; NOT term paper related; NO course topic**
  - Strict time limits 5 mins + 3 mins Q&A; 5 slides (including cover and reference slides: Topic, discussion, conclusion).
- Schedule – as per roster
    - E.g. Genato, Hennes, Jackson, Liu

Security News of the Week



Security News This Week

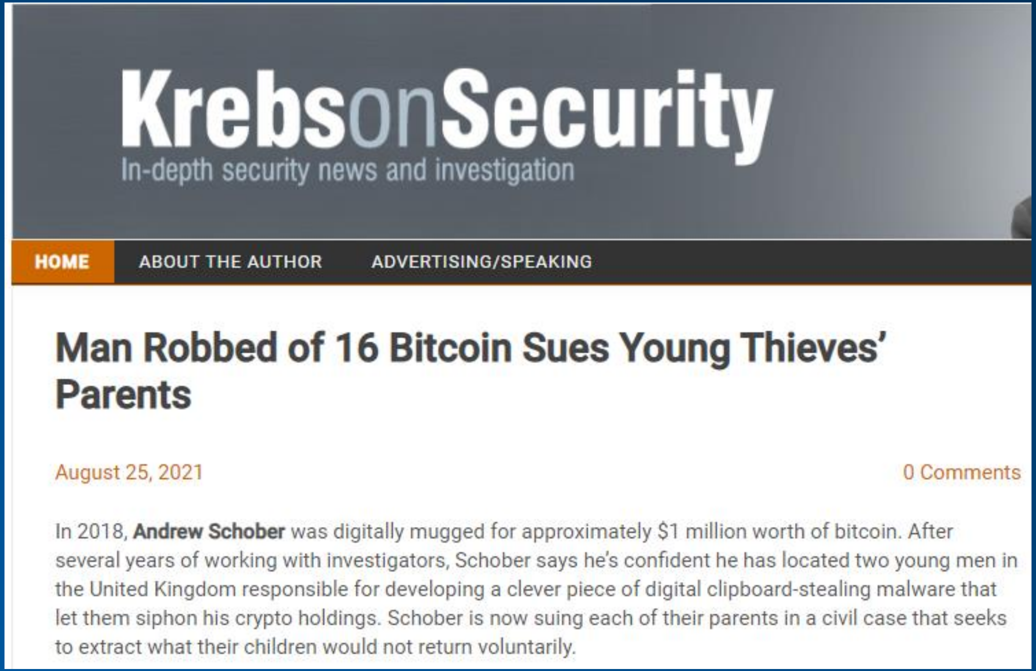
SECURITY ROUNDUP
Google Play Store Has a Malware Problem (Again)
EMILY DREYFUSS

SECURITY ROUNDUP
Trump's North Korea Summit Inspires Spearphishing
EMILY DREYFUSS

SECURITY
T-Mobile Web Portal Exposed 74 Million Accounts
LILY HAY NEWMAN

SECURITY ROUNDUP
Facebook Squashes 19-Year-Old Bug That Still Plagues Web
BRIAN BARRETT

SECURITY THIS WEEK
Security News This Week: Oh Good, Hackers Beat Two-...
WIRED STAFF



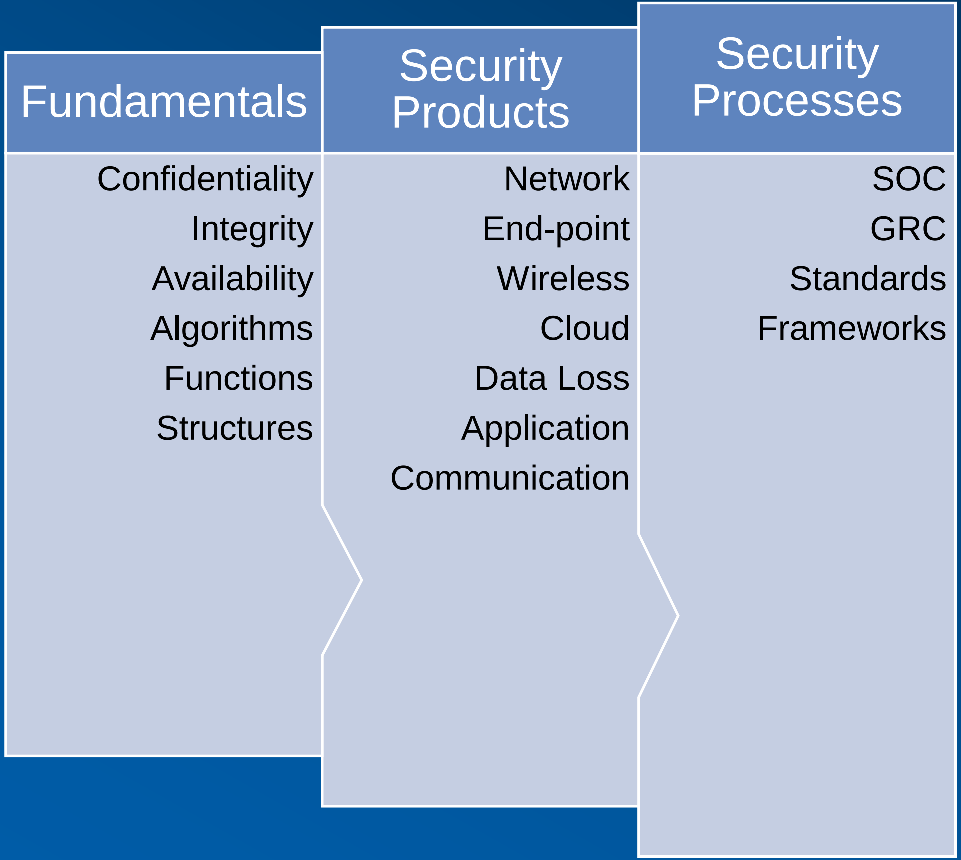
KrebsonSecurity
In-depth security news and investigation

Man Robbed of 16 Bitcoin Sues Young Thieves' Parents

August 25, 2021 0 Comments

In 2018, **Andrew Schober** was digitally mugged for approximately $1 million worth of bitcoin. After several years of working with investigators, Schober says he's confident he has located two young men in the United Kingdom responsible for developing a clever piece of digital clipboard-stealing malware that let them siphon his crypto holdings. Schober is now suing each of their parents in a civil case that seeks to extract what their children would not return voluntarily.

CS7349 – Tying it all together

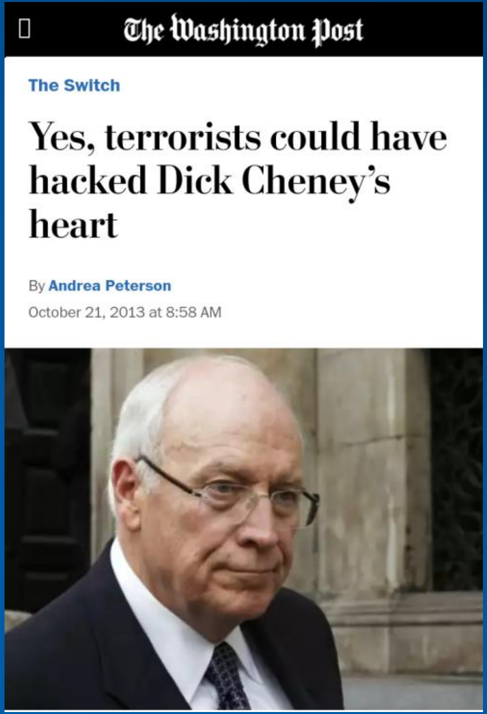


Fundamentals	Security Products	Security Processes
Confidentiality	Network	SOC
Integrity	End-point	GRC
Availability	Wireless	Standards
Algorithms	Cloud	Frameworks
Functions	Data Loss	
Structures	Application	
	Communication	

There are two types of companies: those who have been hacked, and those who don't yet know they have been hacked.

John Chambers
Chief Executive Officer of Cisco

Source: World Economic Forum



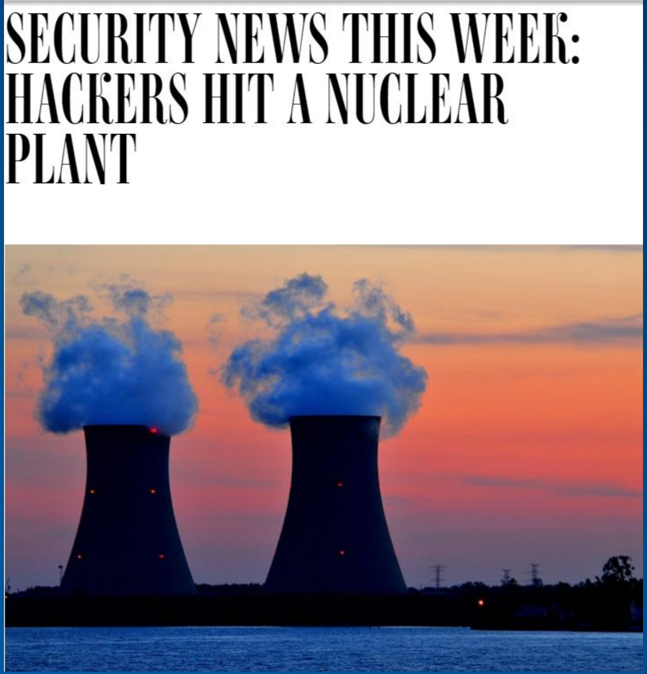
The Washington Post

The Switch

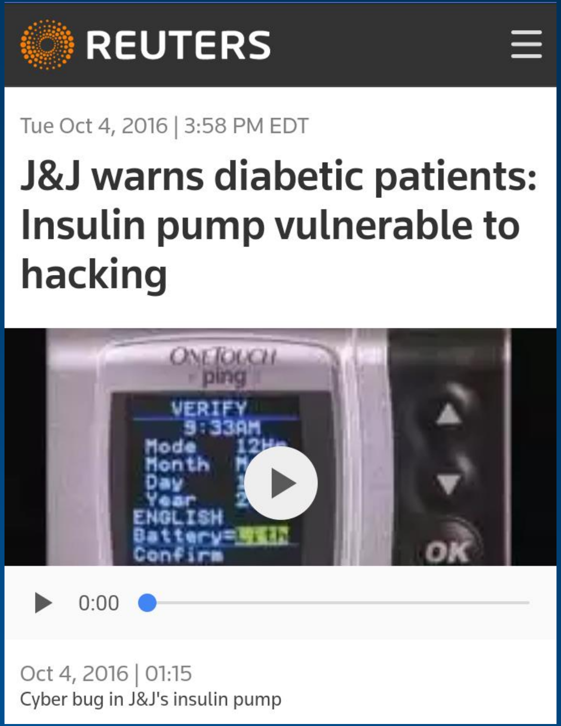
Yes, terrorists could have hacked Dick Cheney's heart

By Andrea Peterson

October 21, 2013 at 8:58 AM



SECURITY NEWS THIS WEEK: HACKERS HIT A NUCLEAR PLANT



REUTERS

Tue Oct 4, 2016 | 3:58 PM EDT

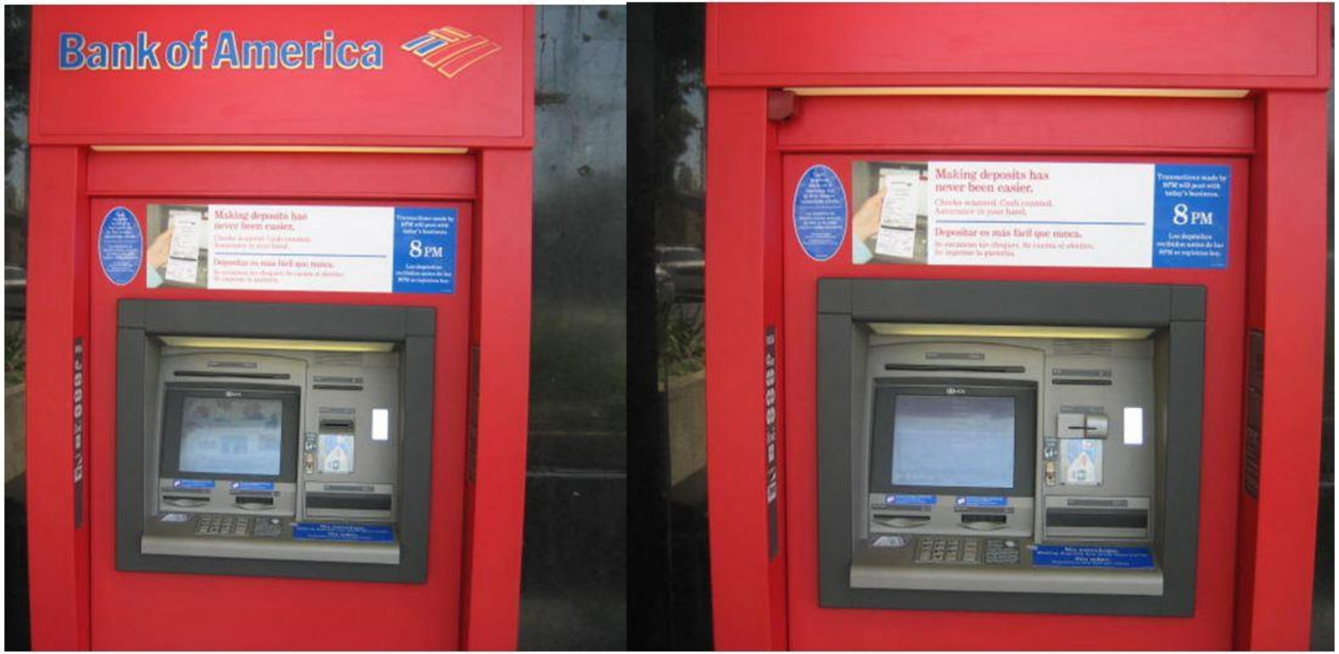
J&J warns diabetic patients: Insulin pump vulnerable to hacking

Oct 4, 2016 | 01:15

Cyber bug in J&J's insulin pump

Sources: Washington Post, Reuters, Wired and Texas Instruments

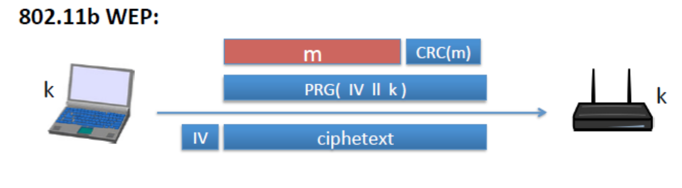
ATM Skimmers


Bank of America
Making deposits has never been easier.
8PM
Making deposits has never been easier.
8PM

WITHOUT

WITH

Wi-Fi Security



- **Wi-Fi: Eavesdropping and Authentication**
  - WEP (Wired Equivalency Protocol). Flawed Security
    - IV = 24 bits; recycles after 2^{24} frames ~ 16M frames; IV resets to 0 after power cycle. AirSnort tool: Opensource tool for breaking WEP key. FBI demo in 2005 (k=104 bits, IV=24 bits). Source: https://crypto.stanford.edu/~dabo/courses/OnlineCrypto/ (Boneh)
    - https://www.sans.org/reading-room/whitepapers/wireless/wireless-networks-security-problems-solutions-172
    - https://www.krackattacks.com/ : Forcing NONCE reuse and Key ReInstallation Attack for WPA2
    - Source: https://www.howtogeek.com/167783/htg-explains-the-difference-between-wep-wpa-and-wpa2-wireless-encryption-and-why-it-matters/

Hacking Cellular Networks - GSM

- **GSM: 1-way authenticates the user to the network and not vice versa.**
    - A5/2 is exploitable with a real-time a ciphertext-only attack
    - A5/1 with a rainbow table attack.

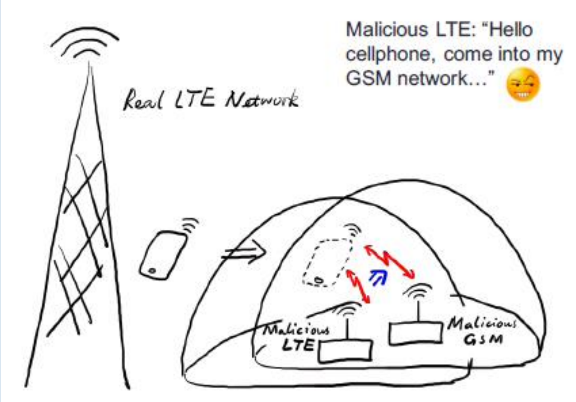
- **Main security concerns regarding with GSM are** :
    - Communications and signaling traffic in the fixed network are not protected.
    - Lawful interception only considered as an after-thought
    - Terminal identity cannot be trusted

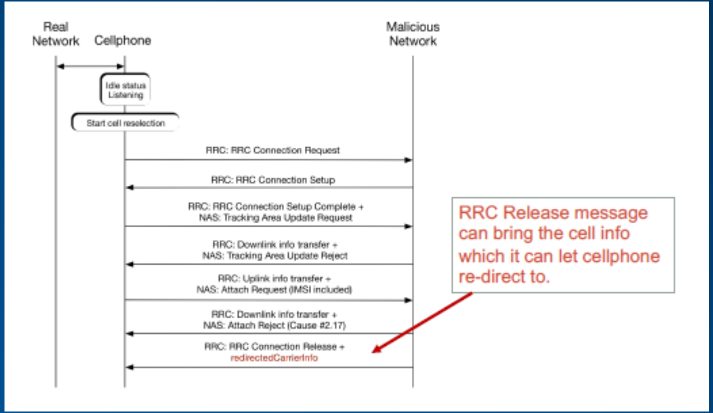
- **Major attacks are:**
    - *Man-in-the-middle attack*.
    - *Eavesdropping*.
    - *Network Impersonation*
    - *User Impersonation*

Source: http://securityaffairs.co/wordpress/1603/security/gsm-mobile-networks.html

Hacking Cellular Networks - LTE

- Redirection-based: Forcing a mobile into a malicious network
- Redirection, DoS (block sms and call)


Malicious LTE: "Hello cellphone, come into my GSM network..."
Real LTE Network
Malicious LTE
Malicious GSM



Real Network

Cellphone

Malicious Network

Idle status Listening

Start cell reselection

RRC: RRC Connection Request

RRC: RRC Connection Setup

RRC: RRC Connection Setup Complete + NAS: Tracking Area Update Request

RRC: Downlink info transfer + NAS: Tracking Area Update Reject

RRC: Uplink info transfer + NAS: Attach Request (IMSI included)

RRC: Downlink info transfer + NAS: Attach Reject (Cause #2.17)

RRC: RRC Connection Release + redirectedCarrierInfo

RRC Release message can bring the cell info which it can let cellphone re-direct to.

- OpenLTE example of open source software for fake LTE network
- **Source:** https://media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/DEFCON-24-Zhang-Shan-Forcing-Targeted-Lte-Cellphone-Into-Unsafe-Network.pdf

Is that possible?? – Fake Towers

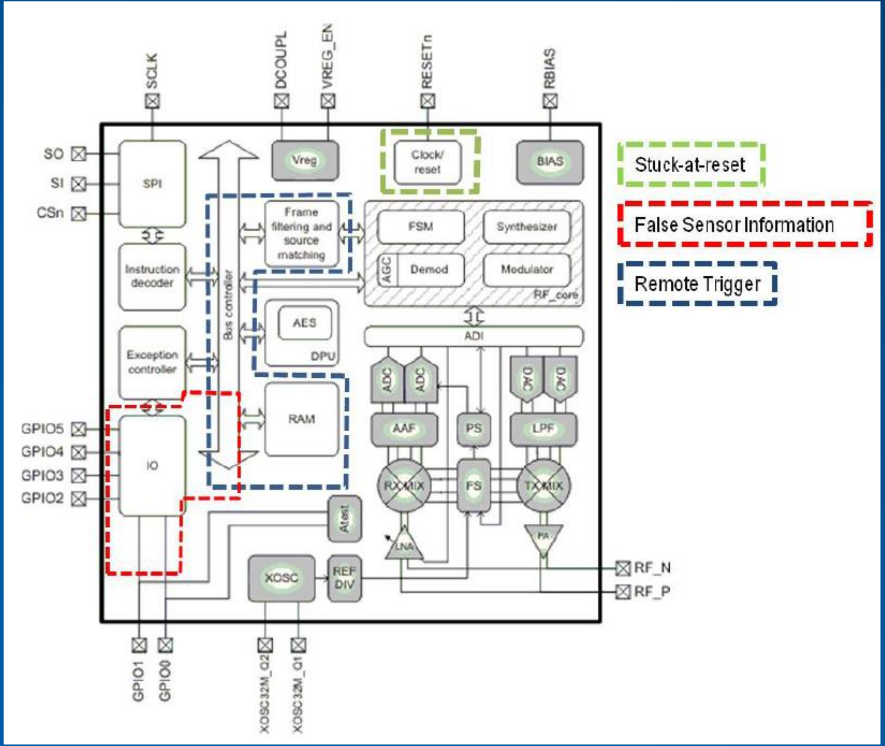
- **Mysterious Phony Cell Towers Intercepting Your Calls?**
  - Every smart phone has a secondary OS, which can be hijacked by high-tech hackers
  - “Interceptors” are usually based near US Military installations or other government sites
  - **https://www.washingtonpost.com/video/business/technology/how-stingray-cellphone-surveillance-devices-work/2018/04/04/62c5f1b4-3db4-11e8-955b-7d2e19b79966_video.html?utm_term=.84e3a97d1d6b**

Source: http://www.popsci.com/article/technology/mysterious-phony-cell-towers-could-be-intercepting-your-calls

Hardware Trojans

- Real Life scenario: Syrian state-of-the-art radar system went “offline” prior to Israeli attack. How?
  - http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch
- Defense Science Board Report: Securing the Cyber Supply Chain. E.g. Counterfeit parts in the F-35 SC
  - https://www.hsdl.org/?view&did=799509
- “How would anyone know if a malicious, remotely controlled circuit had been introduced into a chip?”
- Driven by offshoring of IC foundrys. Reliable supply is not guaranteed for military programs that rely on COTS parts
- https://www.utdallas.edu/~gxm112130/papers/host09.pdf
  - Experiences in Hardware Trojan Design and Implementation

Hardware Trojan possibilities



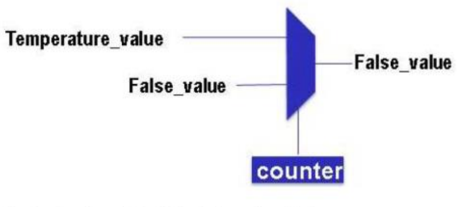
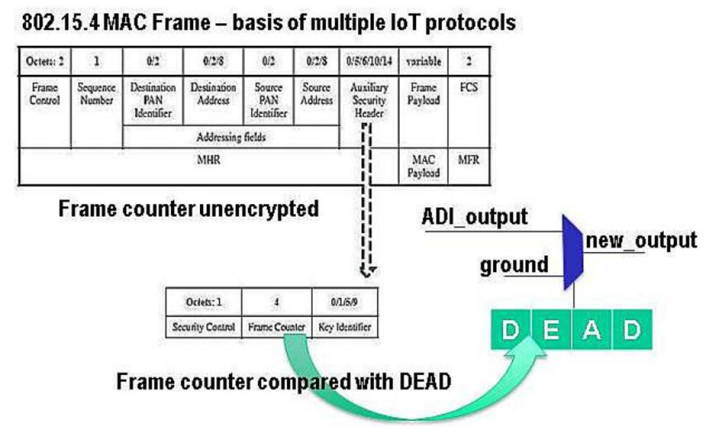


Fig. 5. Design of the False Information Trojan


802.15.4 MAC Frame – basis of multiple IoT protocols

Octets: 2	1	0/2	0/2/8	0/2	0/2/8	0/5/6/10/14	variable	2
Frame Control	Sequence Number	Destination PAN Identifier	Destination Address	Source PAN Identifier	Source Address	Auxiliary Security Header	Frame Payload	FCS
		Addressing fields						
MHR							MAC Payload	MFR

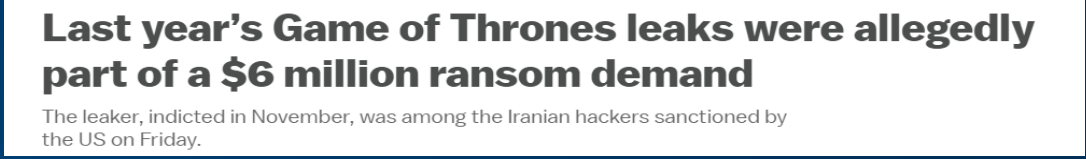
Frame counter unencrypted

Octets: 1	4	0/1/5/9
Security Control	Frame Counter	Key Identifier

Frame counter compared with DEAD

Source: SMU Project on Hardware Trojans in IoT chipset

HBO



Last year’s Game of Thrones leaks were allegedly part of a $6 million ransom demand

The leaker, indicted in November, was among the Iranian hackers sanctioned by the US on Friday.

- Ransom for $6M, later redacted.
  - Leak GoT (Game of Thrones season 7)

I am Mr. Smith and I have the honor to inform you, on behalf of my colleagues, that we successfully breached in your huge network.
[...]
We confess that HBO was one of our difficult targets to deal with but we succeeded. (It took about 6 months).
[...]
By penetrating your Internal Network and other related platforms, we obtained your highly confidential Documents, IT related data, Scripts and etc. these data dump, as you will see, contains HBO’s Various Contracts, Mutual Agreements, Human resources, internal structure, International affiliates, Business strategies, international Marketing, IT infrastructures, producing films & Series (with very detail info!), budget detail for major operations, how you sell and how much!, various strategic insights in every aspects, confidential research, internal letters & Tax Evading Proofs! & Neilsen’s Dirty Job! & etc.
[...]
You concealed GOT7 very carefully so we can’t find it due to lack of time although we are so close. Instead, we produced some tiny mini-series of GOT7 for you which be able to shock the entire world!!! What we got from GOT 7 not only put an end to fate of this season but also corrupts your idea and efforts to season 8.
[...]
Our motives isn’t political nor financial. (Even we hate trump like other Americans do) Its like a game for us, we enjoy to get data. Money isn’t our main purpose.
[...]
(my colleagues argue with me about details given to you and length of this letter, but as there will be very few emails between us, I must assure you about what we have, what will be confronting you and what should be paid to settle down everything!!)
[...]
We honestly share what we got with you and frankly bring you our demand. We are white hat hackers and it’s very shameful if you compare us with some noisy & amateur blackhat ones like Darkoverload. You will see in future steps in our operation that we fulfill any promises made and any given word.

Source: Vox.com

Target

- RAM Scrapers (Target, HD, Albertsons)
  - https://www.wired.com/2014/02/ram-scrapers-how-they-work/ malware that steals CC info and pin, in RAM, at the POS terminal, before encryption. Many types, readily available.

Source: wired.com

Anthem – medical data

- Investigators believe the hackers were from China and had been operating undetected inside the company’s network for months. They gained access by tricking the employee to click on a phishing email that was disguised to look like an internal message. Using the administrator’s credentials, hackers combed through Anthem’s database containing names, social security numbers and birth dates of over 78m people who have been enrolled in its insurance plans since 2004. **(Source: Financial Times)**
- Healthcare records are 10x – 50x more valuable than credit card data. https://networkingexchangeblog.att.com/enterprise-business/healthcare-records-are-50-times-more-valuable-than-credit-ids/

IoT security breaches are increasing

```
Blue Hydra : Devices Seen in last 300s
Queue status: result_queue: 0, info_scan_queue: 1, l
Discovery status timers: 26, ubertooth status: 29
 SEEN | VERS  | ADDRESS              | RSSI ^ | MANUF
  +8s | BTLE  | **:**:26:8A:**:**    |  -65   | Logitec
  +8s | BTLE  | **:**:26:8B:**:**    |  -70   | Logitec
 +17s | BTLE  | **:**:0C:79:**:**    |  -71   | Unknown
 +27s | BTLE  | **:**:16:C4:**:**    |  -73   | Unknown
 +24s | BTLE  | **:**:23:2C:**:**    |  -74   | iBeacon
  +9s | LE4.0 | **:**:C8:F6:**:**    |  -74   | RivieraWaves S.A.S  | 17.78
```

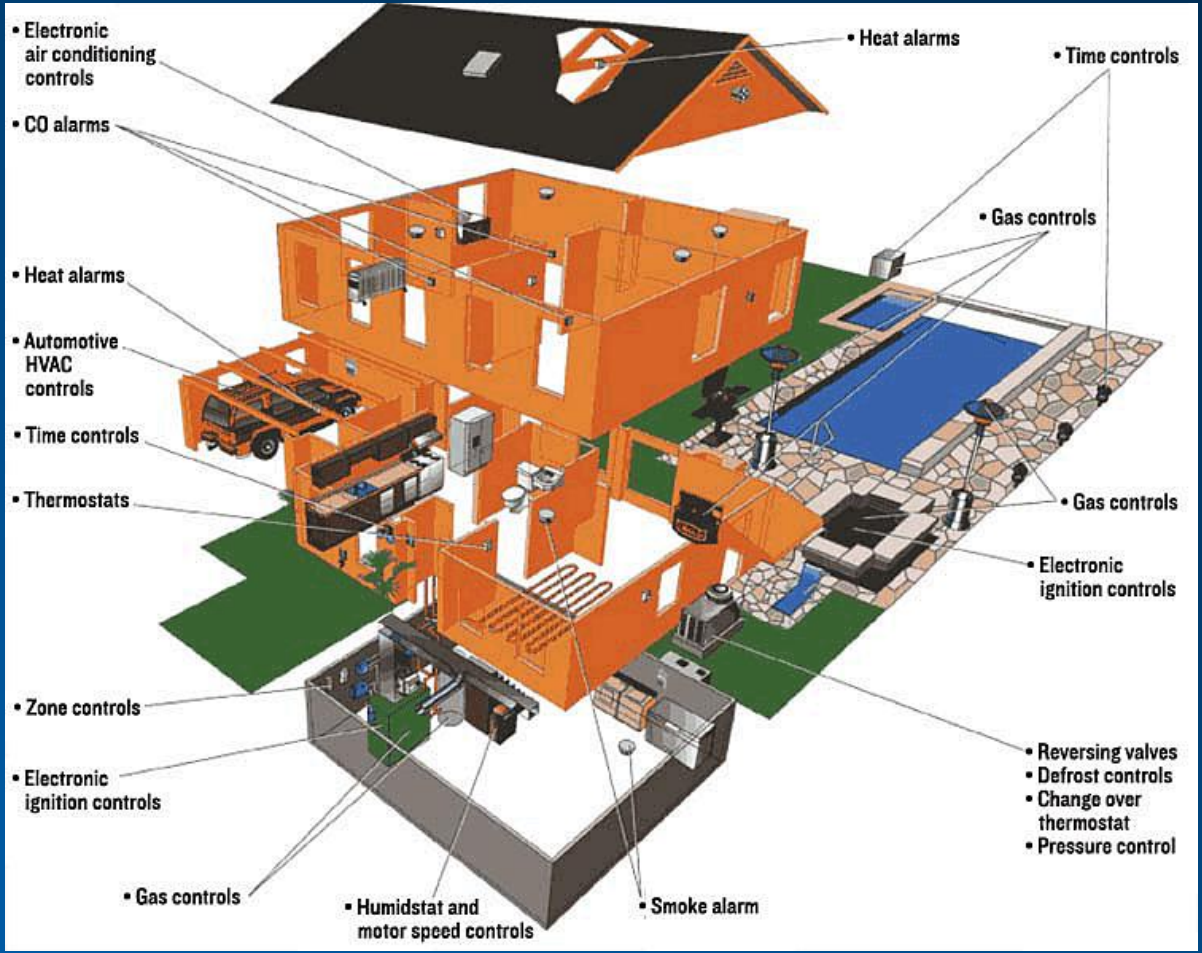
Hacking Smart Locks & IoT Devices

Cameras, Thermostats, and Home Automation Controllers

Hacking 14 IoT Devices

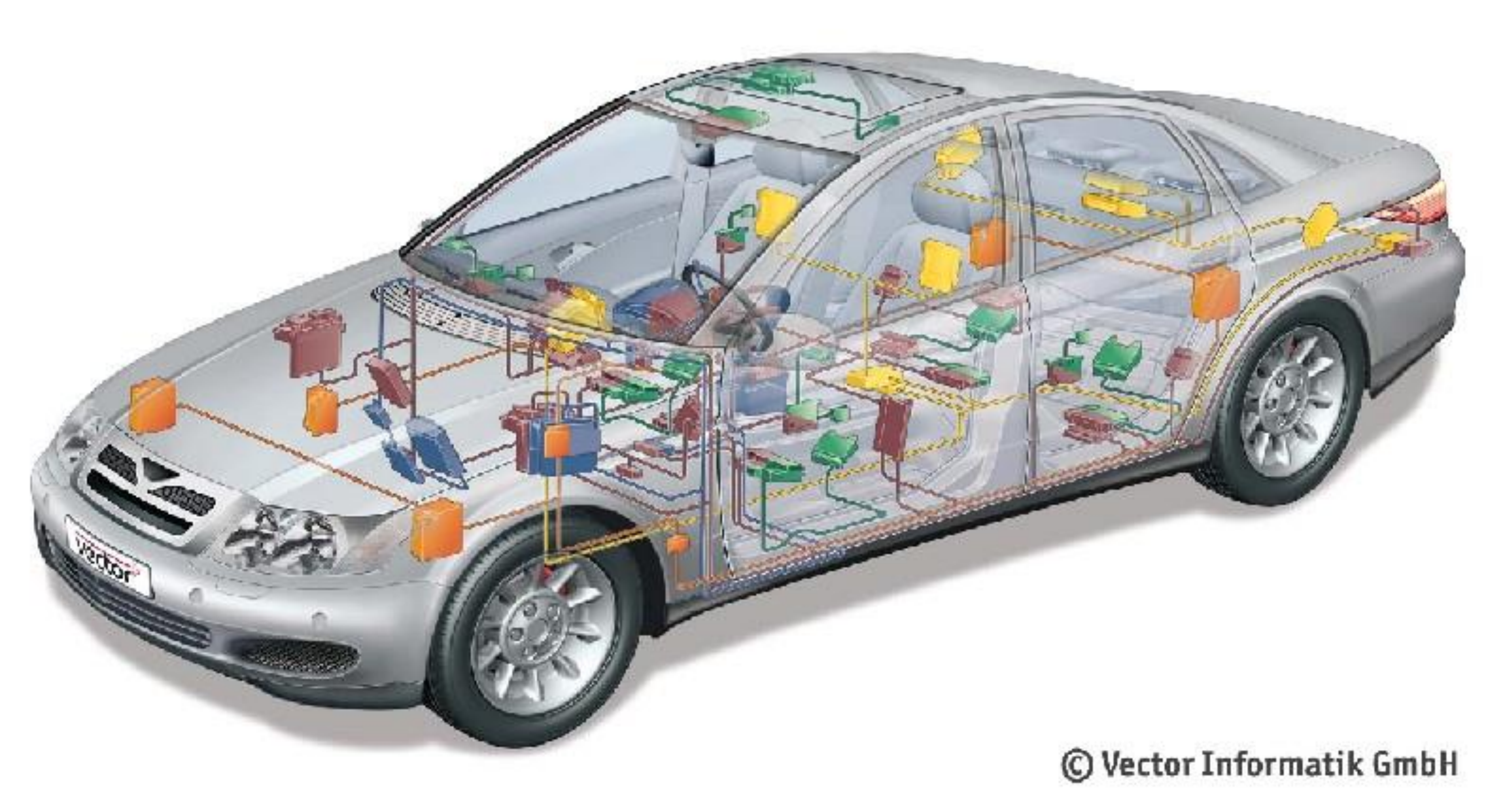
Source: DEF CON Youtube video

Smart Homes



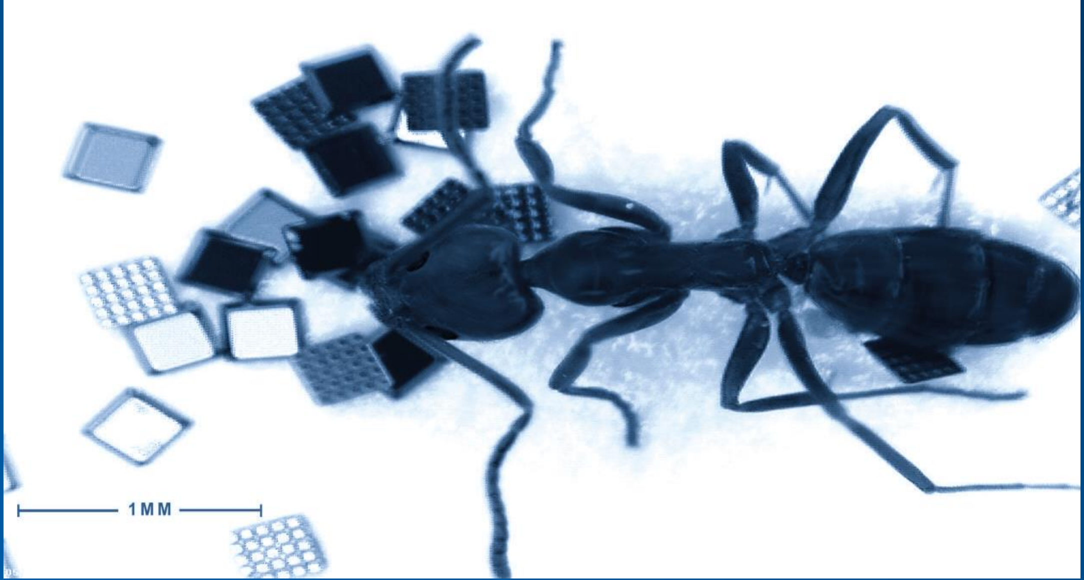
Source: Jon Adams and Bob Heile, “Busy as a ZigBee,” IEEE Spectrum, October 2006

Connected Cars



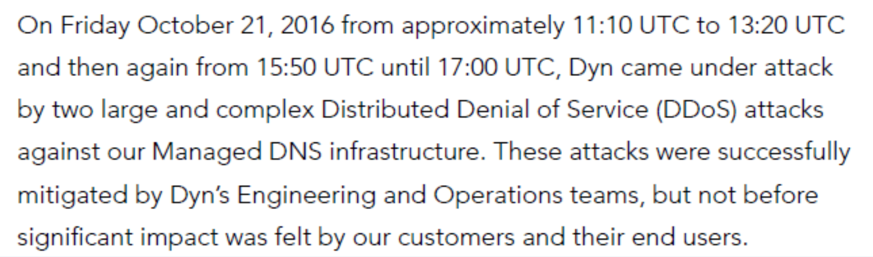
Source: Vector Informatik

Security on a Grain of Sand

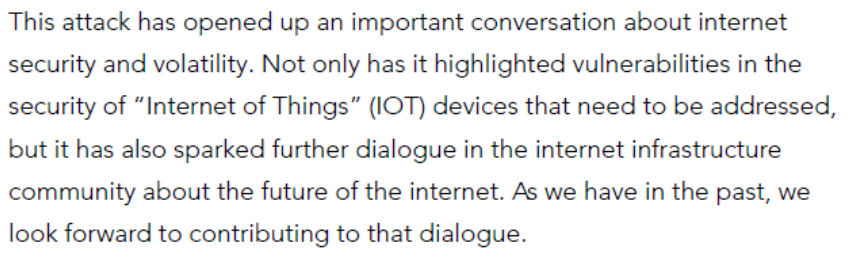


Source: Alien Technology

When IoT attacks the Internet



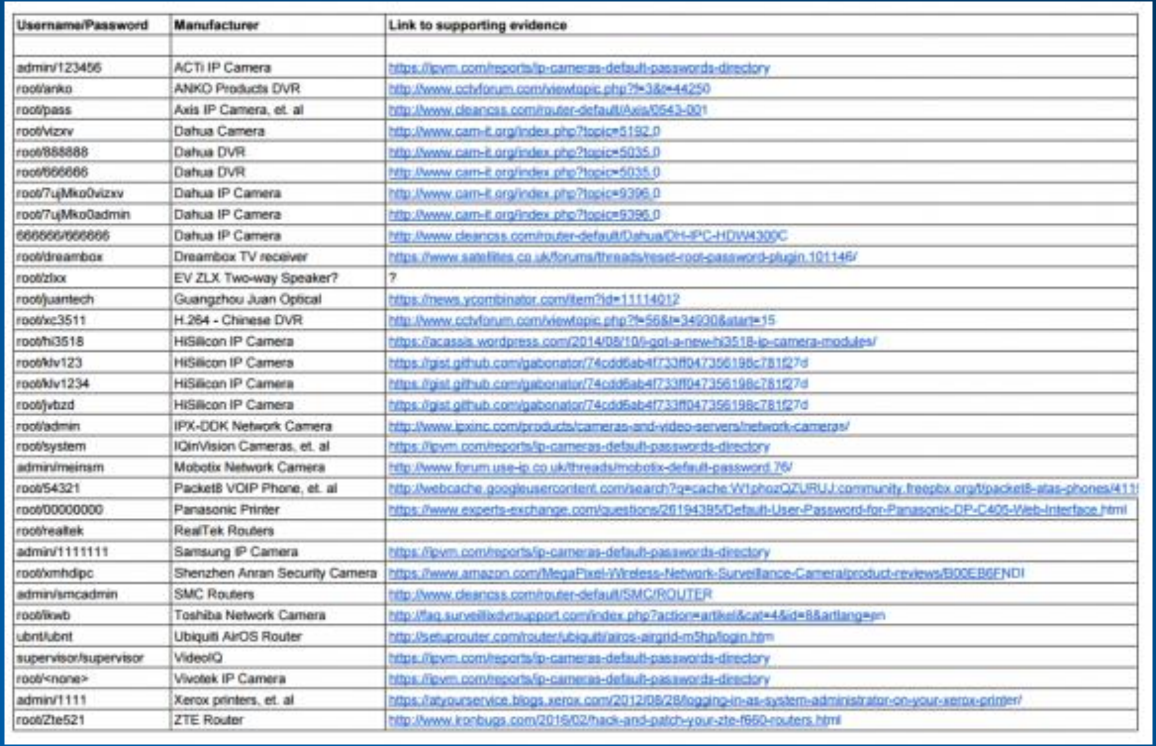
On Friday October 21, 2016 from approximately 11:10 UTC to 13:20 UTC and then again from 15:50 UTC until 17:00 UTC, Dyn came under attack by two large and complex Distributed Denial of Service (DDoS) attacks against our Managed DNS infrastructure. These attacks were successfully mitigated by Dyn's Engineering and Operations teams, but not before significant impact was felt by our customers and their end users.



This attack has opened up an important conversation about internet security and volatility. Not only has it highlighted vulnerabilities in the security of "Internet of Things" (IOT) devices that need to be addressed, but it has also sparked further dialogue in the internet infrastructure community about the future of the internet. As we have in the past, we look forward to contributing to that dialogue.

Source: Oracle Dyn, krebsonsecurity.com

When IoT attacks the Internet



Username/Password	Manufacturer	Link to supporting evidence
admin/123456	ACTi IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/anko	ANKO Products DVR	http://www.cctvforum.com/viewtopic.php?f=3&t=44250
root/pass	Axis IP Camera, et. al	http://www.cleancss.com/router-default/Axis/0543-001
root/vizxv	Dahua Camera	http://www.cam-it.org/index.php?topic=5192.0
root/888888	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/666666	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/7ujMko0vizxv	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
root/7ujMko0admin	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
666666/666666	Dahua IP Camera	http://www.cleancss.com/router-default/Dahua/DH-IPC-HDW4300C
root/dreambox	Dreambox TV receiver	https://www.satellites.co.uk/forums/threads/reset-root-password-plugin.101146/
root/zlxx	EV ZLX Two-way Speaker?	?
root/juantech	Guangzhou Juan Optical	https://news.ycombinator.com/item?id=11114012
root/xc3511	H.264 - Chinese DVR	http://www.cctvforum.com/viewtopic.php?f=56&t=34930&start=15
root/hi3518	HiSilicon IP Camera	https://acassis.wordpress.com/2014/08/10/i-got-a-new-hi3518-ip-camera-modules/
root/klv123	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/klv1234	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/jvbzd	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/admin	IPX-DDK Network Camera	http://www.ipxinc.com/products/cameras-and-video-servers/network-cameras/
root/system	IQinVision Cameras, et. al	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/meinsm	Mobotix Network Camera	http://www.forum.use-ip.co.uk/threads/mobotix-default-password.76/
root/54321	Packet8 VOIP Phone, et. al	http://webcache.googleusercontent.com/search?q=cache:W1phozQZURUJ:community.freepbx.org/t/packet8-atas-phones/411
root/00000000	Panasonic Printer	https://www.experts-exchange.com/questions/26194395/Default-User-Password-for-Panasonic-DP-C405-Web-Interface.html
root/realtek	RealTek Routers	
admin/1111111	Samsung IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/xmhdipc	Shenzhen Anran Security Camera	https://www.amazon.com/MegaPixel-Wireless-Network-Surveillance-Camera/product-reviews/B00EB6FNDI
admin/smcadmin	SMC Routers	http://www.cleancss.com/router-default/SMC/ROUTER
root/ikwb	Toshiba Network Camera	http://faq.surveillixdvrsupport.com/index.php?action=artikel&cat=4&id=8&artlang=en
ubnt/ubnt	Ubiquiti AirOS Router	http://setuprouter.com/router/ubiquiti/airos-airgrid-m5hp/login.htm
supervisor/supervisor	VideoIQ	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/<none>	Vivotek IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/1111	Xerox printers, et. al	https://atyourservice.blogs.xerox.com/2012/08/28/logging-in-as-system-administrator-on-your-xerox-printer/
root/Zte521	ZTE Router	http://www.ironbugs.com/2016/02/hack-and-patch-your-zte-f660-routers.html

Source: Oracle Dyn, krebsonsecurity.com

Deliverables

- Class Participation: 5%
  - Presentation: Any SECURITY topic of your interest: Work, school, play
  - Strict time limits 5 mins + 3 mins Q&A
- Homeworks : HW1 = 10%; Case Study = 10%; HW2 = 10%
- Exams : 30% -exam1 and exam2 – 15% each
- Term Paper – 30% Most important: Form teams NOW!