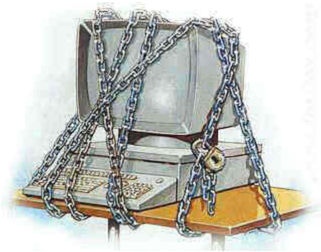
CSCE 665 Advanced Networking & Security

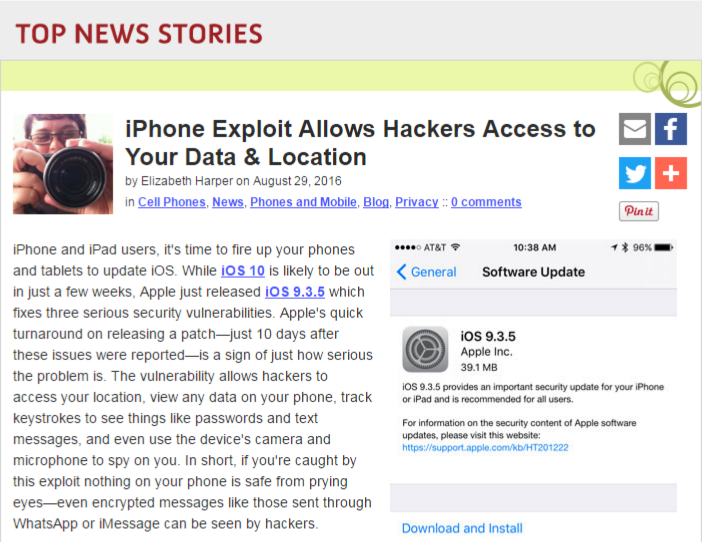
Instructor: Dr. Guofei Gu

http://courses.cse.tamu.edu/guofei/csce665/

Howdy!

- Welcome to the class of studying most recent and real-world security & privacy issues/techniques!
- Background: introduce yourself and your (research) interest/background
  - Let me and other students know more about you
  - To find potential partners to form a team (research project, cyber security compepition…)





TOP NEWS STORIES

iPhone Exploit Allows Hackers Access to Your Data & Location

by Elizabeth Harper on August 29, 2016

in Cell Phones, News, Phones and Mobile, Blog, Privacy :: 0 comments

iPhone and iPad users, it's time to fire up your phones and tablets to update iOS. While iOS 10 is likely to be out in just a few weeks, Apple just released iOS 9.3.5 which fixes three serious security vulnerabilities. Apple's quick turnaround on releasing a patch—just 10 days after these issues were reported—is a sign of just how serious the problem is. The vulnerability allows hackers to access your location, view any data on your phone, track keystrokes to see things like passwords and text messages, and even use the device's camera and microphone to spy on you. In short, if you're caught by this exploit nothing on your phone is safe from prying eyes—even encrypted messages like those sent through WhatsApp or iMessage can be seen by hackers.

●●●●○ AT&T 10:38 AM 96%

< General Software Update

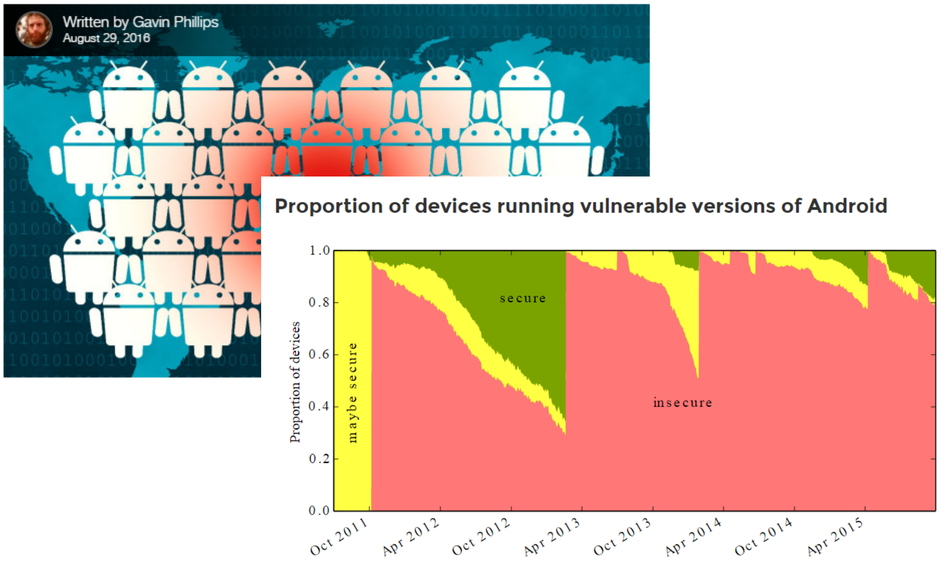
iOS 9.3.5
Apple Inc.
39.1 MB

iOS 9.3.5 provides an important security update for your iPhone or iPad and is recommended for all users.

For information on the security content of Apple software updates, please visit this website:
https://support.apple.com/kb/HT201222

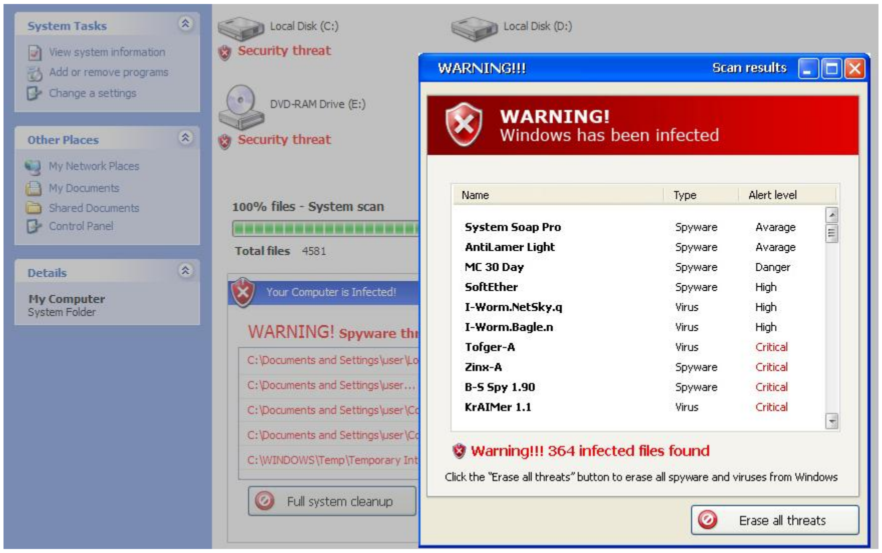
Download and Install

Are You One Of 900 Million Android Users Exposed By QuadRoot?



This figure shows our estimate of the proportion of Android devices running *insecure*, *maybe secure* and *secure* versions of Android over time. Further details on how this figure constructed can be found on a separate page.

http://androidvulnerabilities.org/



100% files - System scan

Total files 4581

Your Computer is Infected!

WARNING! Spyware thr

C:\Documents and Settings\user\Lo
C:\Documents and Settings\user...
C:\Documents and Settings\user\Co
C:\Documents and Settings\user\Co
C:\WINDOWS\Temp\Temporary Int

WARNING!
Windows has been infected

Name	Type	Alert level
System Soap Pro	Spyware	Avarage
AntiLamer Light	Spyware	Avarage
MC 30 Day	Spyware	Danger
SoftEther	Spyware	High
I-Worm.NetSky.q	Virus	High
I-Worm.Bagle.n	Virus	High
Tofger-A	Virus	Critical
Zinx-A	Spyware	Critical
B-S Spy 1.90	Spyware	Critical
KrAIMer 1.1	Virus	Critical

Warning!!! 364 infected files found

Click the "Erase all threats" button to erase all spyware and viruses from Windows

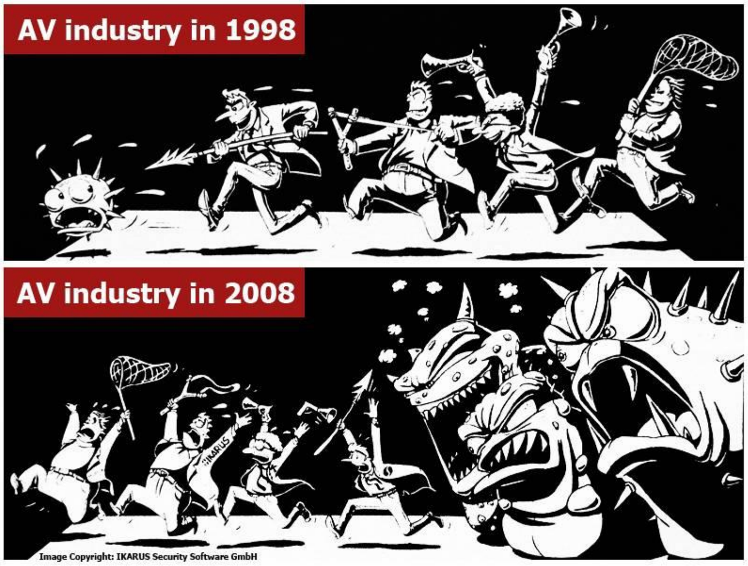


Image Copyright: IKARUS Security Software GmbH

What is Security?

- [Informally] Security is the *prevention* of certain types of *intentional* actions from occurring
  - These potential actions are **threats**
  - Threats that are carried out are **attacks**
  - Intentional attacks are carried out by an **attacker**
  - Objects of attacks are **assets**

Goals of Security

Prevention

- Prevent attackers from violating security policy

Detection

- Detect attackers’ violation of security policy

Recovery

- Stop attack, assess and repair damage

Survivability

- Continue to function correctly even if attack succeeds

Components of Security

Confidentiality

- Keeping data and resources hidden. Privacy.

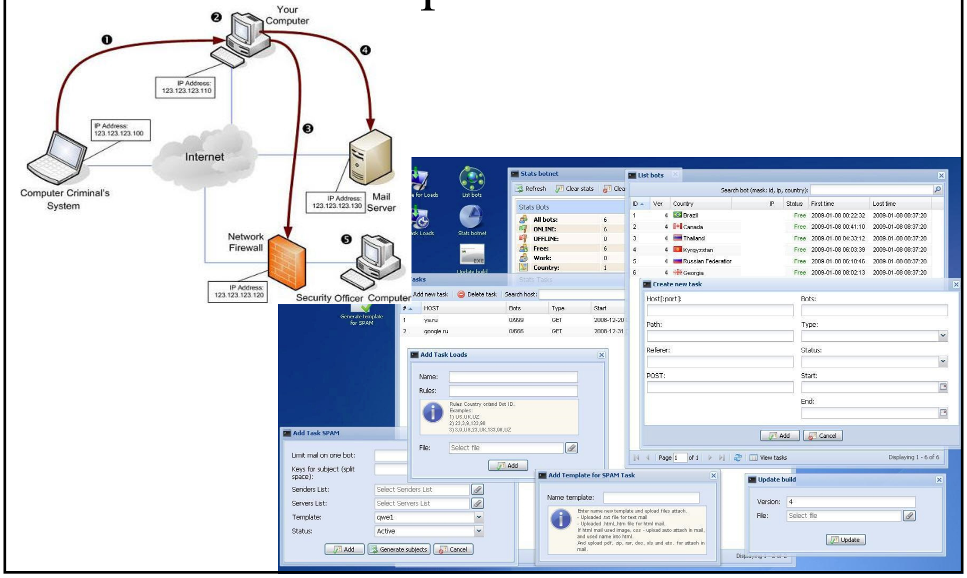
Integrity

- Preventing unauthorized changes to data or resources.

Availability

- Enabling access to data and resources

Example: Botnet


Your Computer
❷
❶
❹
IP Address: 123.123.123.110
❸
IP Address: 123.123.123.100
Internet
Computer Criminal's System
IP Address: 123.123.123.130
Mail Server
Network Firewall
❺
IP Address: 123.123.123.120
Security Officer Computer
List bots
Stats botnet
Update build
Generate template for SPAM
Refresh
Clear stats
Add
Generate subjects
Cancel
Update

Stats botnet

Stats Bots

All bots:	6
ONLINE:	6
OFFLINE:	0
Free:	6
Work:	0
Country:	1

List bots

Search bot (mask: id, ip, country):

ID	Ver	Country	IP	Status	First time	Last time
1	4	Brazil		Free	2009-01-08 00:22:32	2009-01-08 08:37:20
2	4	Canada		Free	2009-01-08 00:41:10	2009-01-08 08:37:20
3	4	Thailand		Free	2009-01-08 04:33:12	2009-01-08 08:37:20
4	4	Kyrgyzstan		Free	2009-01-08 06:03:39	2009-01-08 08:37:20
5	4	Russian Federatior		Free	2009-01-08 06:10:46	2009-01-08 08:37:20
6	4	Georgia		Free	2009-01-08 08:02:13	2009-01-08 08:37:20

Tasks

Add new task · Delete task · Search host:

#	HOST	Bots	Type	Start
1	ya.ru	0/999	GET	2008-12-20
2	google.ru	0/666	GET	2008-12-31

Create new task

Host[:port]: · Bots: · Path: · Type: · Referer: · Status: · POST: · Start: · End:

Add Task Loads

Name: · Rules:

Rules Country or/and Bot ID.
Examples:
1) US,UK,UZ
2) 23,3,9,133,98
3) 3,9,US,23,UK,133,98,UZ

File: Select file

Add Task SPAM

Limit mail on one bot:
Keys for subject (split space):
Senders List: Select Senders List
Servers List: Select Servers List
Template: qwe1
Status: Active

Add Template for SPAM Task

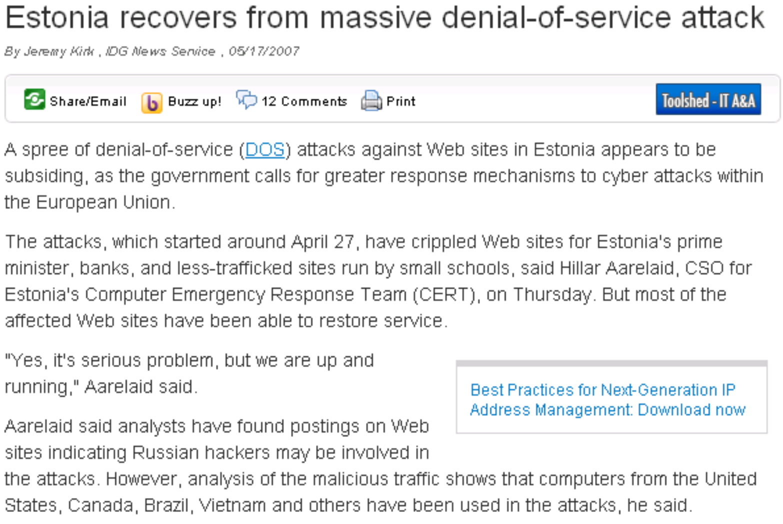
Name template:

Enter name new template and upload files attach.
- Uploaded .txt file for text mail
- Uploaded .html,.htm file for html mail.
If html mail used image, css - upload auto attach in mail, and used name into html.
And upload pdf, zip, rar, doc, xls and etc. for attach in mail.

Update build

Version: 4
File: Select file

Denial of Service



Estonia recovers from massive denial-of-service attack

By Jeremy Kirk , IDG News Service , 05/17/2007

A spree of denial-of-service (DOS) attacks against Web sites in Estonia appears to be subsiding, as the government calls for greater response mechanisms to cyber attacks within the European Union.

The attacks, which started around April 27, have crippled Web sites for Estonia's prime minister, banks, and less-trafficked sites run by small schools, said Hillar Aarelaid, CSO for Estonia's Computer Emergency Response Team (CERT), on Thursday. But most of the affected Web sites have been able to restore service.

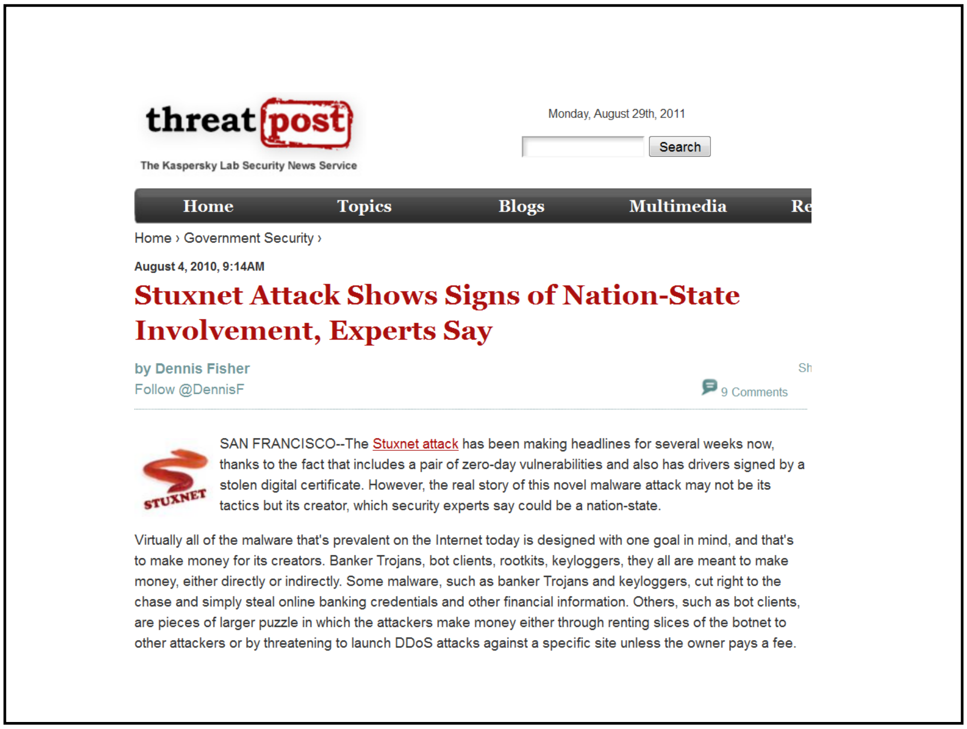
"Yes, it's serious problem, but we are up and running," Aarelaid said.

Aarelaid said analysts have found postings on Web sites indicating Russian hackers may be involved in the attacks. However, analysis of the malicious traffic shows that computers from the United States, Canada, Brazil, Vietnam and others have been used in the attacks, he said.

Malware

More…

- “Attack of the tweets: Major Twitter Flaw Exposed” – UK researcher says vulnerability in Twitter API lets an attacker take over a victim’s account – with a tweet. Aug 27, 2009 [Darkreading]
- Conficker worm



threatpost
The Kaspersky Lab Security News Service
Monday, August 29th, 2011
Search
Home
Topics
Blogs
Multimedia
Re
STUXNET

Home › Government Security ›

August 4, 2010, 9:14AM

Stuxnet Attack Shows Signs of Nation-State Involvement, Experts Say

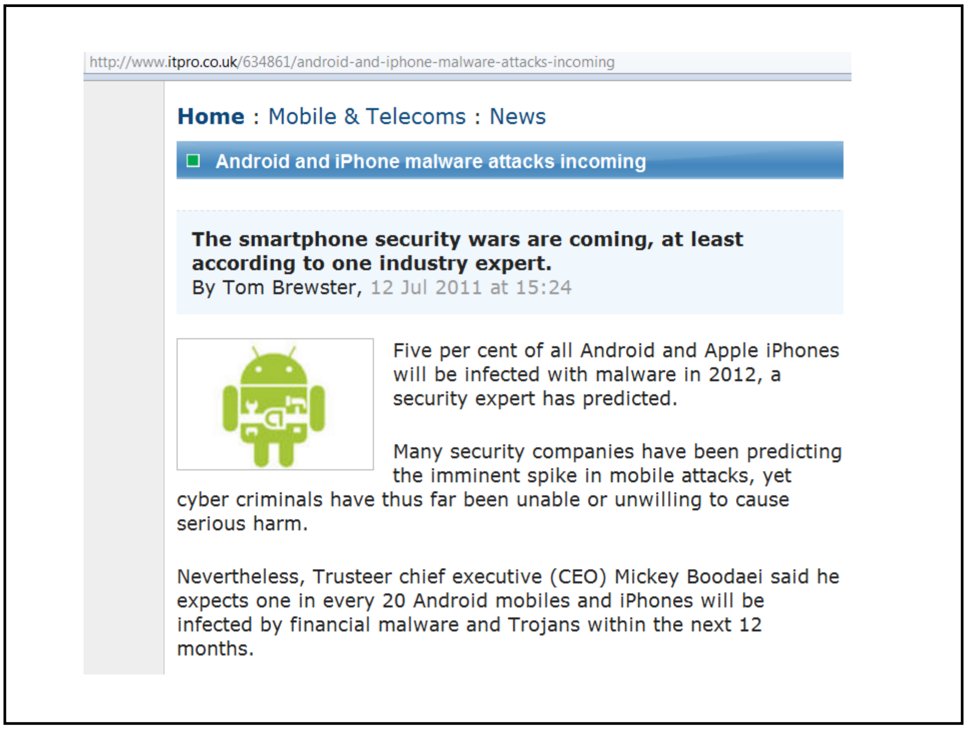
by Dennis Fisher
Follow @DennisF

Sh

9 Comments

SAN FRANCISCO--The Stuxnet attack has been making headlines for several weeks now, thanks to the fact that includes a pair of zero-day vulnerabilities and also has drivers signed by a stolen digital certificate. However, the real story of this novel malware attack may not be its tactics but its creator, which security experts say could be a nation-state.

Virtually all of the malware that's prevalent on the Internet today is designed with one goal in mind, and that's to make money for its creators. Banker Trojans, bot clients, rootkits, keyloggers, they all are meant to make money, either directly or indirectly. Some malware, such as banker Trojans and keyloggers, cut right to the chase and simply steal online banking credentials and other financial information. Others, such as bot clients, are pieces of larger puzzle in which the attackers make money either through renting slices of the botnet to other attackers or by threatening to launch DDoS attacks against a specific site unless the owner pays a fee.



http://www.itpro.co.uk/634861/android-and-iphone-malware-attacks-incoming

Home : Mobile & Telecoms : News

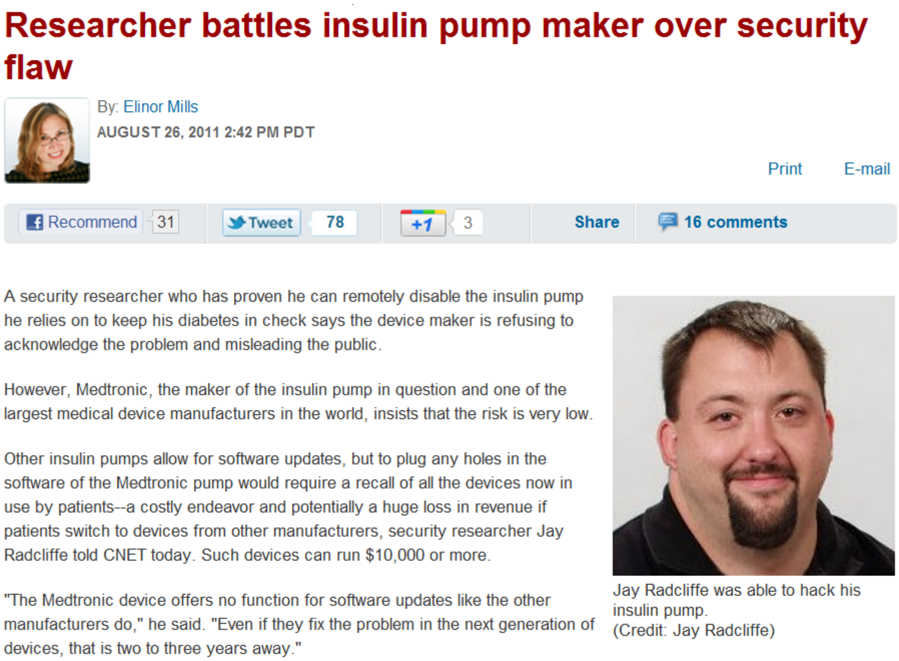
Android and iPhone malware attacks incoming

The smartphone security wars are coming, at least according to one industry expert.
By Tom Brewster, 12 Jul 2011 at 15:24

Five per cent of all Android and Apple iPhones will be infected with malware in 2012, a security expert has predicted.

Many security companies have been predicting the imminent spike in mobile attacks, yet cyber criminals have thus far been unable or unwilling to cause serious harm.

Nevertheless, Trusteer chief executive (CEO) Mickey Boodaei said he expects one in every 20 Android mobiles and iPhones will be infected by financial malware and Trojans within the next 12 months.



Researcher battles insulin pump maker over security flaw

By: Elinor Mills

AUGUST 26, 2011 2:42 PM PDT

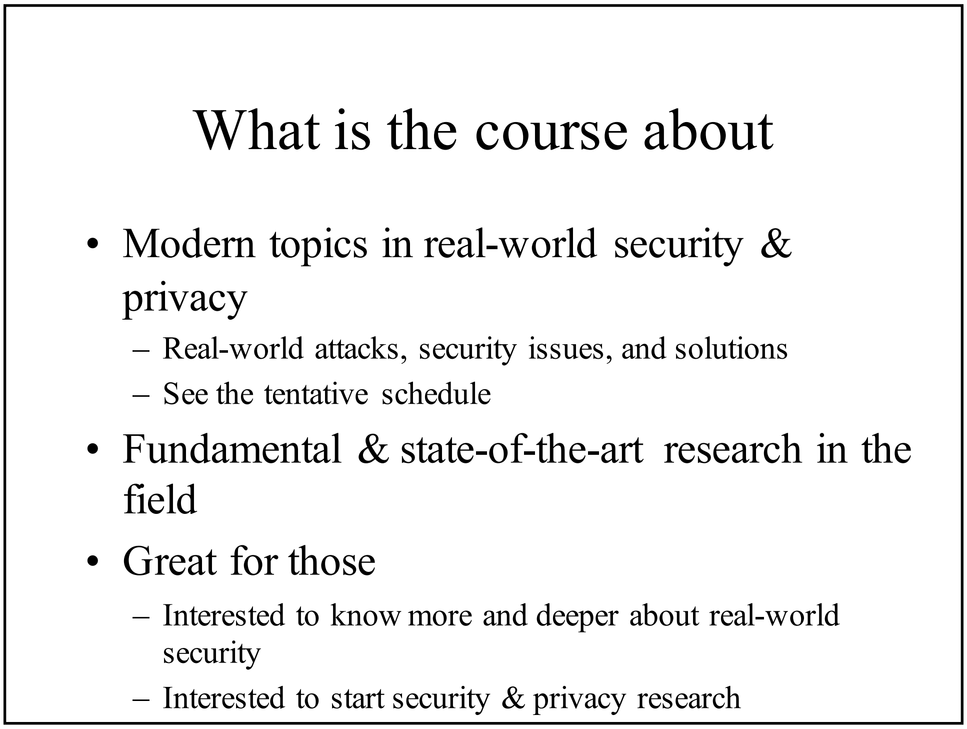
A security researcher who has proven he can remotely disable the insulin pump he relies on to keep his diabetes in check says the device maker is refusing to acknowledge the problem and misleading the public.

However, Medtronic, the maker of the insulin pump in question and one of the largest medical device manufacturers in the world, insists that the risk is very low.

Other insulin pumps allow for software updates, but to plug any holes in the software of the Medtronic pump would require a recall of all the devices now in use by patients--a costly endeavor and potentially a huge loss in revenue if patients switch to devices from other manufacturers, security researcher Jay Radcliffe told CNET today. Such devices can run $10,000 or more.

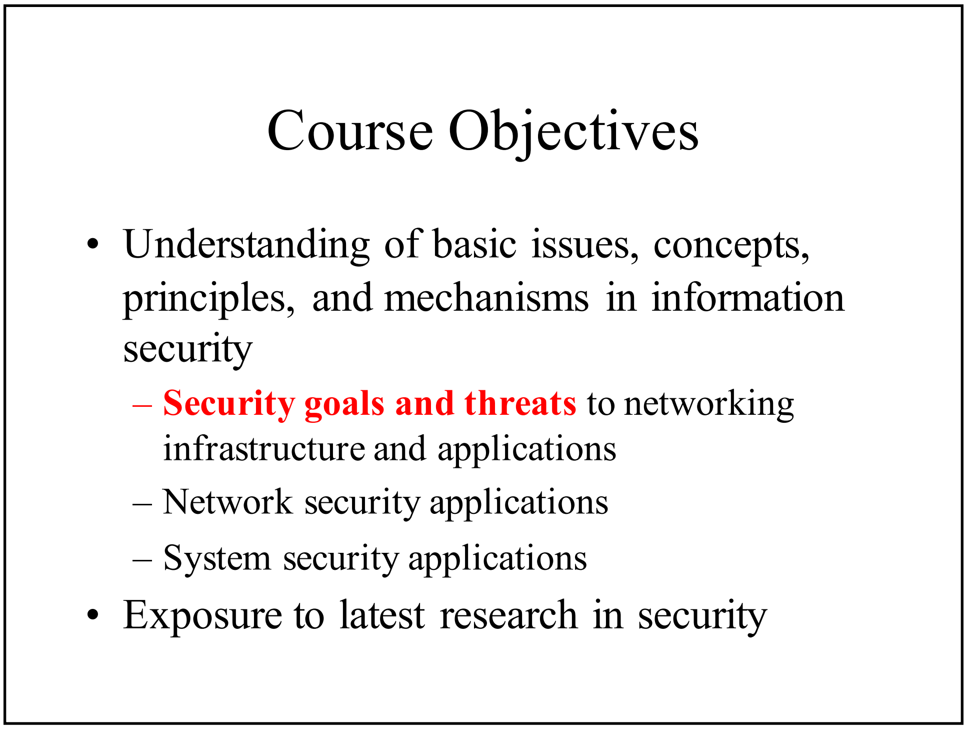
"The Medtronic device offers no function for software updates like the other manufacturers do," he said. "Even if they fix the problem in the next generation of devices, that is two to three years away."

Jay Radcliffe was able to hack his insulin pump.
(Credit: Jay Radcliffe)



What is the course about

- Modern topics in real-world security & privacy
  - Real-world attacks, security issues, and solutions
  - See the tentative schedule
- Fundamental & state-of-the-art research in the field
- Great for those
  - Interested to know more and deeper about real-world security
  - Interested to start security & privacy research



Course Objectives

- Understanding of basic issues, concepts, principles, and mechanisms in information security
  - **Security goals and threats** to networking infrastructure and applications
  - Network security applications
  - System security applications
- Exposure to latest research in security

Goals & Non-goals

- Goals
  - Explore range of current problems and tensions in modern computer security
  - Understand how to identify security issues in your own research and how to address them
  - Figure out if security is an area of interest for you
  - Get feet wet in security research (lab, mini project)
- Non-goals
  - Review of all std security mechanisms
  - Significant examination of applied cryptography

Topics may be covered in this course

- Network security: such as Worm, IDS, botnet, SDN/OpenFlow security
- System security: such as malware analysis/defense, virtualization for security, information flow, smartphone security
- Application security: such as web security, spam

Prerequisites

- Networking, operating systems, and programming (C or C++ or Java)
- The **right** motivation
- Warning: this is NOT an easy course!

Textbook

- Most readings will be from research papers in top security conferences and journals
- Recommended (but not required) textbook for more background learning
  - [KPS] Charlie Kaufman, Radia Perlman, and Mike Speciner. *Network Security—Private Communication in a Public World*, 2nd Edition. Prentice Hall, 2002. ISBN 978-0-13-046019-6.
  - [PP] Charles P. Pfleeger and Shari Lawrence Pfleeger. Security in Computing, 5th Edition. Prentice Hall, 2015. ISBN 0134085043.
  - [SB] William Stallings and Lawrie Brown. Computer Security: Principles and Practice, 3rd Edition. Prientice Hall, 2014. ISBN 0133773922.
  - [GT] Michael Goodrich and Roberto Tamassia. Introduction to Computer Security, Addison-Wesley, 2010. ISBN 0321557867

Grading

- Paper presentation/mini-review and class participation: 20%
- Homework: 30%
- Mini research project: 50%
- (No middle/final exams)

All late submissions within one day will lose 40% credit!
Submissions later then two days are NOT accepted!

Paper Presentation/mini-review

- You will do a paper presentation (slides upon approval 2 days before presentation) and/or do mini-reviews (for the classes with student presentations)
- Mini-review should at least include:
  - A short summary of the paper (should not simply copy the abstract!). Make the problem/motivation/idea/technique/result very clear.
  - Why the paper is good? List at least two things you like the paper (i.e., pros/merits).
  - What are the problems/limitations of the paper? List at least three things you think the paper can improve (i.e., cons/limitations).
  - Literature review (be clear and *concise*): what are the main related/competitive studies? how does this paper distinguish itself?
  - What can you do based on this work: lessons learned from this work? stimulate any new related problem? flawed assumption/technique can be improved/extended? any technique can be used to other (maybe your own dedicated) domain to solve other problem? what extension can you do for further work? ...

Homework

- You will be asked to finish instructed assignments/labs by yourself and submit necessary reports.
  - – Some homework will be related to network security
  - – Some homework will be related to malware analysis/defense (e.g., botnet, honeynet trace analysis)
  - – Some homework will be related to SDN app development

Mini Research Project

- Semester long; Team up or individual!
- Implementation/measurement/analysis, and evaluation of an interesting idea on some security topic (not necessarily covered in the course, maybe related to your own research area)
- Submit: a workshop quality report
- BONUS points for excellent projects!

Mini Research Project (cont.)

- You project can be one or more likely some combination of the following (in any case, the idea should be interesting!)
  - Analysis
  - Measurement
  - Development/implementation
  - Algorithm design (with clear application)
  - New attack
  - Replicate/improve an important research tool
- Process
  - Topic selection (upon approval): think now and talk to me ASAP
  - Proposal (with literature review)
  - Status report
  - Presentation
  - Final report
- The grade will be based on novelty, depth, correctness, clarity of presentation, and effort.
- There will be a people's choice best project award at end!

Random Ideas on Project

- Privacy in social networking applications
- Security in twitter-like micro blog systems
- Security in facebook-like social networking websites
- Security analysis/attack in iPhone/Android/itouch/Wii/PS3/Xbox
- Automatic monitoring & analysis of underground economic on IRC/website/…
- Cloud security (Software/platform/Infrastructure as a service)

Random Ideas on Project

- Wireless (WLAN/Cellular/Adhoc/Sensor) security
- Security issues in online game
- Malware analysis: how to extract C&C protocols? Behavior? New unpacking?
- Security attack and analysis of AJAX systems (e.g., Gmail, googlemap)
- Massive spam or phishing study: URL analysis, content analysis, temporal analysis, network-level analysis, new spam approach? collection

Random Ideas on Project

- Web security (browser, server); web intrusion detection
- Improving Network Security with OpenFlow (software defined networking)
- New botnet detection technique; evasion hardness analysis; high-speed botnet detection
- Click fraud study and detection
- Web bot detection and defense
- DNS security: fast flux, scam hosting, domain monitoring, cache poisoning

Random Ideas on Project

- Cryptography: new attack on new cryptosystems; application to new domain to solve new problems?
- Information flow tracking in network? in Internet? In social networking application? Other new application domains?
- New application of virtualization for security?
- New DDoS attack & defense techniques?
- Security issues in Cyber-Physic System
- Study of censorship on Internet; anti-censorship techniques and systems

Other Issues

- Ethics
- Master thesis project

- Look at the topics/papers in the tentative schedule
- Think about your project now!