Internet Security: A Reality Check

Dirceu Cavendish

Kyushu Institute of Technology

Outline

- Security Concepts
- Authentication Mechanisms
- Encryption
- Data Harvesting
- Cloud Computing
- Future Applications

Network Design Research Center

Security – 20+ years of threats

Welcome to [Your Favorite Mainframe] System

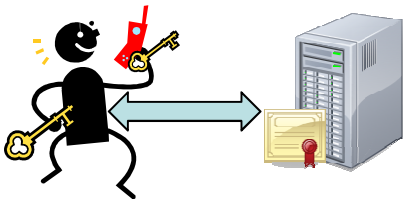
USERNAME:
PASSWORD:

Failed to login

- Server spoofing
- Password leakage
- Client spoofing
- OS security bypass

Security Concepts

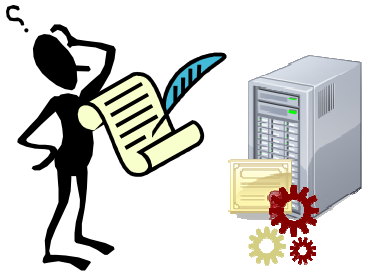
- Client/Server Communication
- Cryptography
  - Ciphers
  - Cryptographic keys
  - Key derivation functions
- Mutual Authentication
  - Credentials
  - Protocols

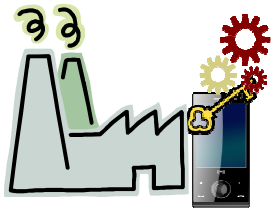


Network Design Research Center

Key Management

- Key Delivery
- Key Storage and Retrieval
- Safe Cipher Execution



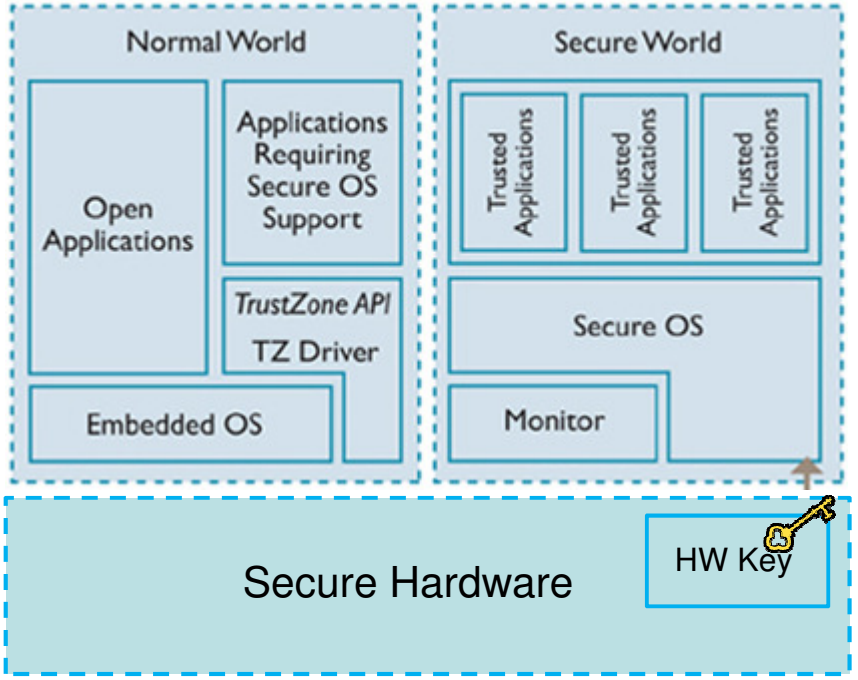


Network Design Research Center

Secure High-Level OS

Independent and customized OS for security

- Secure HW access
- Secure booting
- Secure file system
- Secure cipher execution



Network Design Research Center

Server target attacks

Opera Software – June 2013

- Password stealing malware
- Installs as legitimate Opera Software
- Use Opera stolen Certificate

Bit9 Security Firm – Feb 2013

- Code-signing certificate stolen
- Bit9 provides security to US Gov and Fortune 500 companies

Stuxnet – How to crash a nuclear reactor

- Windows vulnerabilities
- USB infection
- Use stolen certificate to replace driver
- Spoofs control signals to monitoring system

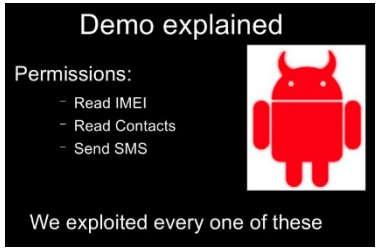
"Organizations' failure to control and protect cryptographic keys and certificates, the foundation of digital security and online trust, leaves the front doors open for attackers to enter at will and pilfer whatever sensitive data they want, whenever they want," said Jeff Hudson, CEO of key management company Venafi, who added that most companies aren't clear on their inventory of keys and certificates.
"Unplanned outages from expired certificates can no longer be viewed as an inconvenient IT operations issue, rather these common outages are symptomatic of much larger security vulnerabilities," Hudson said. "It's become clear that certificate-based attacks have become the attack vector of choice. Organizations must implement effective controls to ensure the safety of their network."

"I guess if you're a bad guy trying to get malware installed on a computer at a hardened target that is using Bit9, what choice do you have except going through Bit9 first?" Grossman said. "This is not the result of some mass malware blast. This is almost certainly highly targeted."

Data Harvesting

User controlled permission

- Easy to bypass



Third party controlled

- Network operators (e.g. device management software)
- Service providers (e.g. social networks)
- E-commerce (e.g. recommendation engines)

May 2013 - Surveys on Retail Personalization Technology Can't Justify Data Collection Invasion of Privacy - Will Shoppers Opt Out as Legal Retail Cyber Spying Grows?

How long did you spend inside the store each time you visited? Where did you walk inside the store? What merchandise displays did you pause in front of? How long did you spend in the dressing room? Did you walk past our store and walk into a competitor's store? How much time did you spend there? All of this information might have been gathered and shared about you the last time you visited a mall.

July 2013 - New revelations about the U.S. spying programs show officials from the Federal Bureau of Investigation and several U.S. government departments have been interfering with commercial agreements in order to secure access to fiber-optic networks.

The Washington Post reported on Sunday that lawyers form the FBI and the departments of Defense, Justice, and Homeland Security demanded an operator of fiber-optic networks to maintain an internal corporate cell of American citizens with government clearances after selling those cables to an Asian firm.

June 2013 - Facebook said Friday it fixed a bug that exposed contact info for over six million accounts. The admission revealed its 'shadow profile' data collection activities, and users are furious.

Network Design Research Center

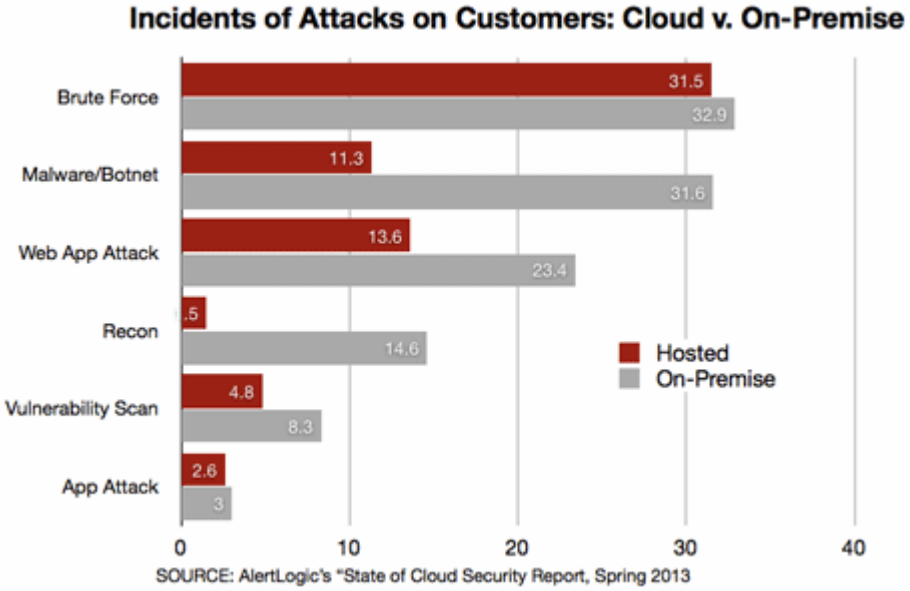
Cloud Computing

Secure clouds

- Cloud data protection
- Customer isolation
- Web application access control
- Data access management

What should customers ask

- Who manages your data
- Regulatory compliance
- Where is your data hosted
- Data segregation technology
- Data recovery mechanism
- Data forensic technology
- Long term data hosting viability



Network Design Research Center

Medical Systems

Secure medical services

- Patient monitoring
- Remote medical assistance
- Data privacy
- Service reliability

Jan 2013 - A pair of researchers best known for poking holes in industrial control systems (ICS) products found that medical devices suffer similar security woes after they were able to easily hack into a Philips medical information management system that directly interfaces with X-ray machines and other medical devices.

Turns out there is some overlap vendor-wise with electronic medical devices and ICS products: Siemens, Philips, Honeywell, and GE all provide products to both industries. The system and other medical device security problems mirror some of the same types of shortcomings Rios and McCorkle have seen firsthand with ICS products, the researchers say.

BLACK HAT USA 2011 -- Las Vegas -- A security researcher at Black Hat yesterday demonstrated how a hacker could remotely turn off a diabetic person's insulin pump without his knowledge. The findings came after months of research delving into the security of the portable medical devices that monitor diabetics' blood-sugar levels and those that deliver the body-chemistry-balancing insulin necessary to keep those levels in check throughout the day.

Network Design Research Center

Internet of Things

Ubiquitous P2P communication

- Authentication
- Safe key storage on small footprint hardware
- Scalable key management
  - Large scale key provisioning and credential revocation

July 2012 - At the Black Hat security conference Tuesday evening, a Mozilla software developer and 24-year old security researcher named Cody Brocious plans to present a pair of vulnerabilities he's discovered in hotel room locks from the manufacturer Onity, whose devices are installed on the doors of between four and five million hotel rooms around the world according to the company's figures. Using an open-source hardware gadget Brocious built for less than $50, he can insert a plug into that DC port and sometimes, albeit unreliably, open the lock in a matter of seconds. "I plug it in, power it up, and the lock opens," he says simply.

The system's vulnerability arises, Brocious says, from the fact that every lock's memory is entirely exposed to whatever device attempts to read it through that port. Though each lock has a cryptographic key that's required to trigger its "open" mechanism, that string of data is also stored in the lock's memory, like a spare key hidden under the welcome mat. So it can be immediately accessed by Brocious's own spoofed portable device and used to open the door a fraction of a second later.

IOT security "kit"!

Network Design Research Center

Summary

Internet Security Reality Check

- Internet security protocols are not trouble free
  - Cipher suits must be constantly checked against breaches.
  - Security protocols rely on premises that may be violated.
- Security weaknesses are dealt with via multiple approaches.
  - Certificates plus IP address/machine checking plus UN/PW
  - Attacks are becoming more multi-layered and targetted
- New applications/systems will require fresh security approaches
  - New security hardware modules
  - New/scalable authentication methods
  - New technologies to support attack forensics

Network Design Research Center