Trust and IT Security

Artem Kazantsev
Sr. Security Analyst
@DukeITSO
security@duke.edu
http://security.duke.edu

Duke
UNIVERSITY

What is IT Security?

- C onfidentiality
- I ntegrity
- A vailability

Duke
UNIVERSITY

What is “trust”?

- Feeling or emotion?
- State of relationships?
- Information concept?
- All of the above?

Duke
UNIVERSITY

Who do you trust?

In real life,

- Do we trust people?
- Do we trust business?
- Do we trust government(s)?

Duke
UNIVERSITY

How do we build trust?

- Small “transactions” (bridge building)
- Reliability
- Consistency
- Always mutual
  building from
- “Web of trust”
  to
- “Society of trust”

Duke
UNIVERSITY

“What's in your wallet?”

As an illustration of trust, let's take a monetary transaction:

- Cash in $$$? Cash in other currency?
- Credit Cards?
- Driver's License?
- Duke Card?
- Coupons?

Duke
UNIVERSITY

Trust and Risk

- If you trust someone, can you eliminate risk completely?
- Societies built around families vs societies built around civic communities: is trust an issue?
- Historical examples: Allies of World War II; 1890 British Ultimatum (England / Portugal)
- ???

Duke
UNIVERSITY

Enter technology...

- From human tellers to ATMs
- From in-person to online banking
- From cashiers to self-service express lines in grocery stores
- From brick-and-mortar stores to online shopping
- From on-campus to online education

human interactions are becoming rare...

Duke
UNIVERSITY

How does technology changes trust relationships?

Authentication of parties: making sure we are dealing with the “right” entity

- Identity management systems (who has the system of record?)
- Digital Certificates (what is SSL lock and how Man-in-the-Middle attack works)
- Multi-factor authentication (debit cards, smart phones, biometrics)

Duke
UNIVERSITY

How trust can be undermined?

- Fraud
  - Misrepresentation
  - Impersonation
- Deception
- Any other criminal activity we can think of...
- Remember “reliability” and “consistency”? Anything unreliable and inconsistent will undermine the trust

Duke
UNIVERSITY

Explicit trust for IT transactions: what do we assume should be trusted?

- Root Certification Authorities
- Software distribution
- Background checks for employees
- Government approved standards (NIST)
- Transactions integrity

Duke
UNIVERSITY

Why that is not always the case...

- Root Certification Authorities – certificates are compromised by exploitation of weak algorithms
- Software distribution – compromised by backdoor installation in websites
- Background checks for employees – not always done, and not helpful for ongoing psychological evaluations
- Government approved standards (NIST) – new leaks from Edward Snowden are suggesting
  NSA advocating using weak encryption algorithms
- Transactions integrity – the presence of a third party (a hacker, a government agency) negates the one-to-one secrecy of transactions

Duke
UNIVERSITY

Compare and contrast

- Businesses are “hacked” all the time.
  - Consider the latest Adobe compromise: 2.9 Million customers were affected AND source code was stolen
  - Do you trust Adobe products less as a result of this compromise? (yes / no)? Why?
- NSA is circumventing much of the encryption that protects vast amounts of information on the Web
  - Do you feel online transactions are secure?
  - Can you trust your privacy is intact online?

Duke
UNIVERSITY

The role of the IT security

Bruce Schneier: *"Security exists to facilitate trust. Trust is the goal, and security is how we enable it." (February 23, 2012)*

Duke
UNIVERSITY

Counterpoint

Security is a tool that helps maintaining trust

if it is already established, but cannot build it

if it does not exist or repair it if it's damaged

Duke
UNIVERSITY

Trust no one? Or...

- Put pressure on the vendors to
  - Disable weak encryption
  - Be more transparent about your privacy and consumer data usage
- Put pressure on the government to stop unwarranted wiretaps and interceptions, stop NSA surveillance programs, revamp FISA court legislation

Duke
UNIVERSITY

Educate users...

- Combat phishing, educate your friends, coworkers, relatives and kids
- Use multifactor authentication on campus and and at home
- Promote strong encryption for data at rest and in motion

Duke
UNIVERSITY

Questions?

- artem.kazantsev@duke.edu
- security@duke.edu
- http://security.duke.edu
- @DukeITSO

Duke
UNIVERSITY