Mobile Banking
Understanding the Risks

Randy Romes, CISSP, CRISC, MCP, PCI-QSA
Principal
CliftonLarsonAllen LLP
Information Security Services

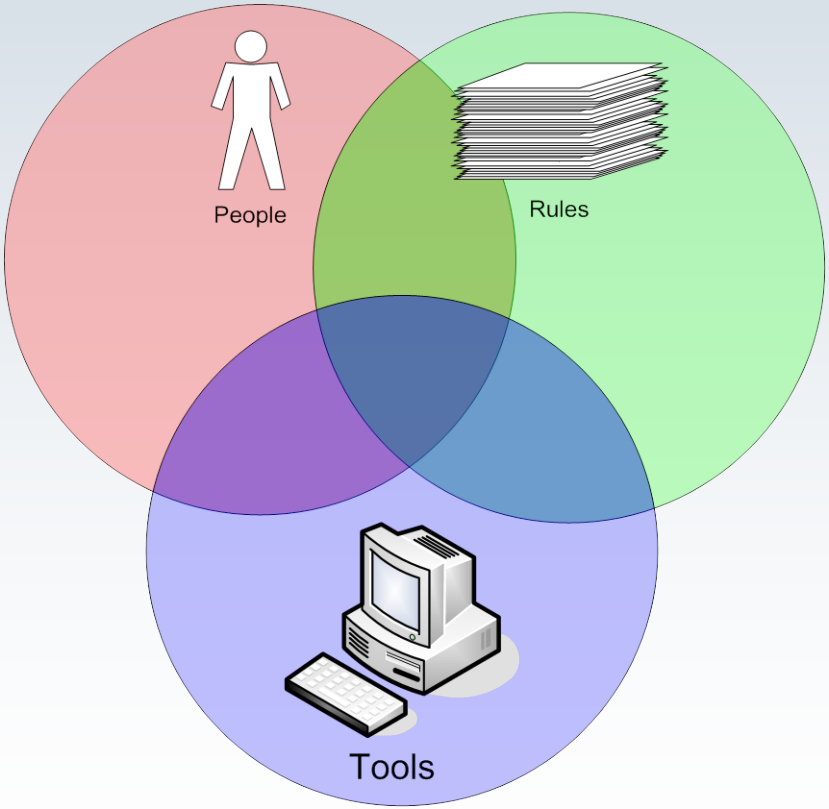
Overview

- Mobile Banking Basics
- Vulnerabilities, Risks, and Controls
- Vendor Management
- Compliance

Definition of a Secure System

"A secure system is one we can depend on to behave as we expect."

Source: "Web Security and Commerce" by Simson Garfinkel with Gene Spafford



- Confidentiality
- Integrity
- Availability

Mobile Banking Basics

- Mobile Banking is here to stay…
- More people have (smart) phones than computers
  - 4 billion mobile phones
  - 3 billion are SMS enabled
  - 1 billion are smartphones
- Mobile payments are coming (already here?)
  - Topic for another time

Mobile Banking Basics

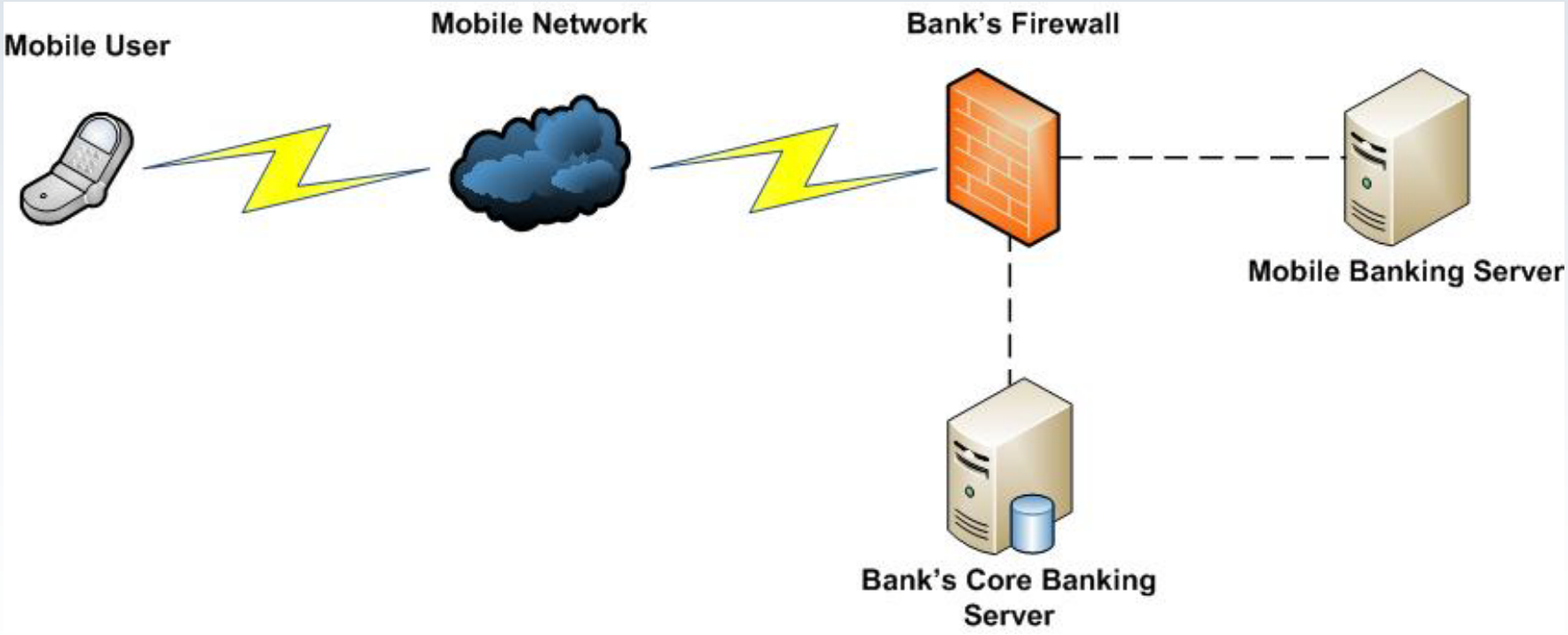
- Different types of mobile banking
  - SMS mobile banking
  - Mobile web
  - Mobile applications

Mobile Banking Basics

- Mobile banking applications (i.e. “mobile apps”)
  - Various mobile app market places
  - iTunes/Apple App Store
  - Android Market
  - Verizon App Store
  - BlackBerry App Store

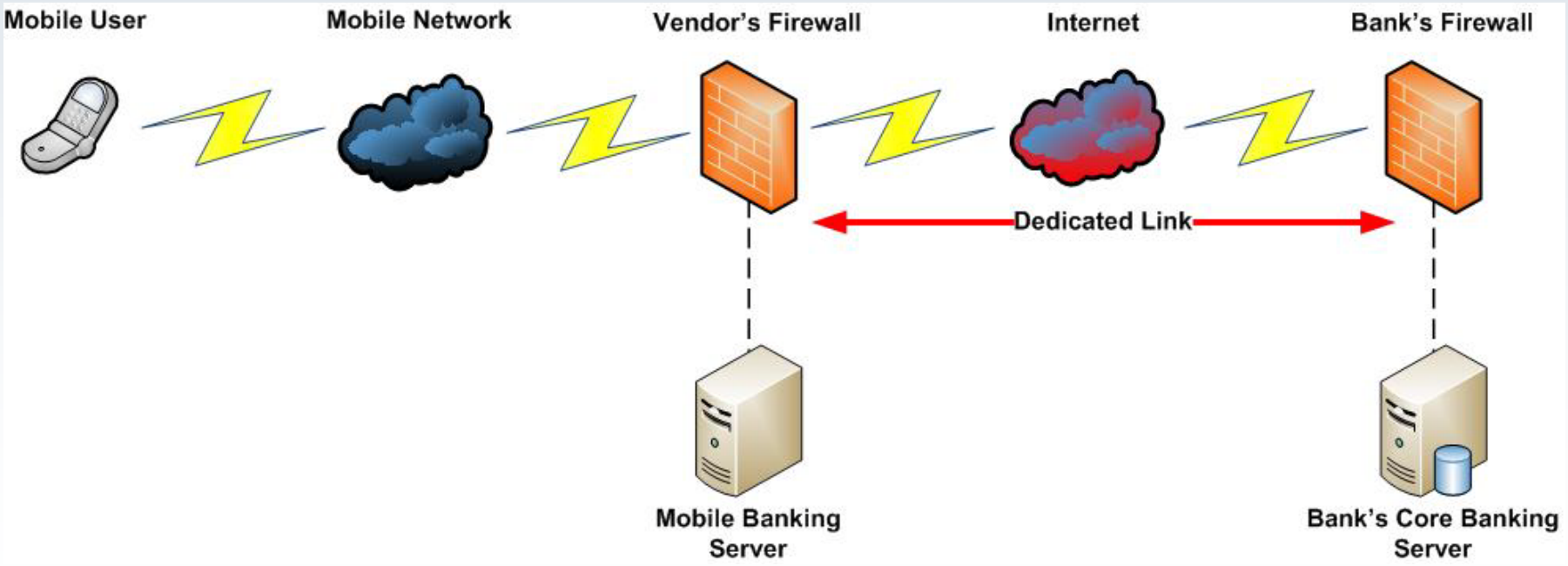
Mobile Banking Basics

- Basic/common mobile banking infrastructure
  - Mobile banking system at the bank



Mobile Banking Basics

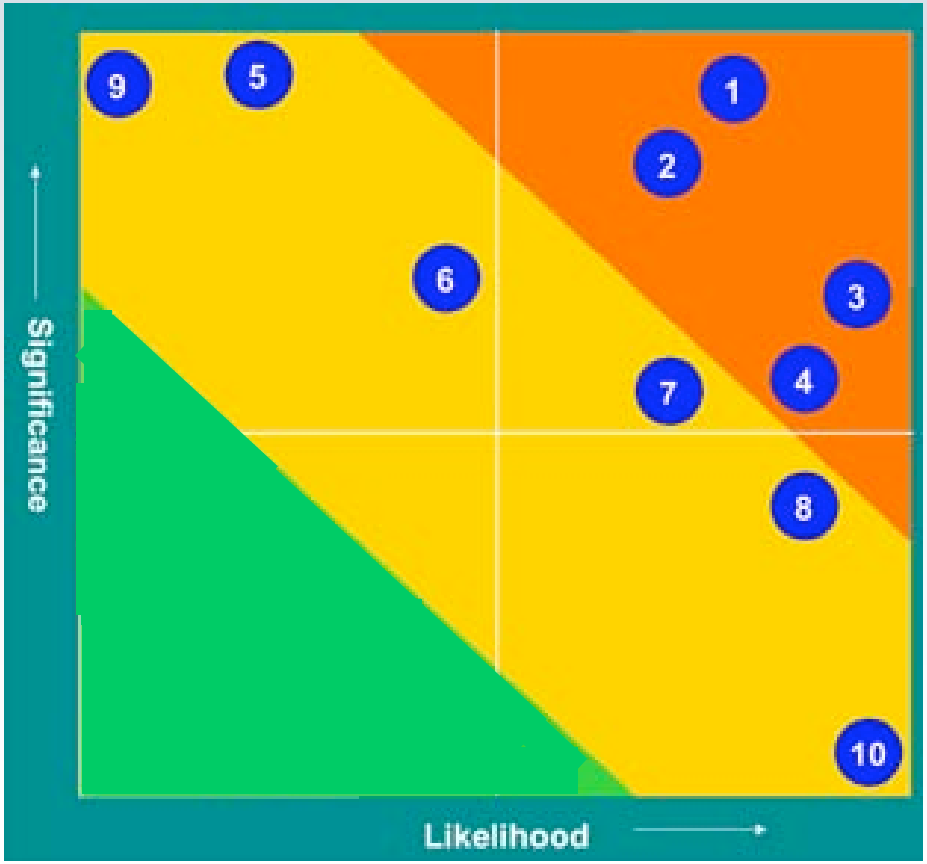
- Basic/common mobile banking infrastructure
  - Mobile banking system with third party vendor between customer and bank infrastructure



Vulnerabilities, Risks, & Controls

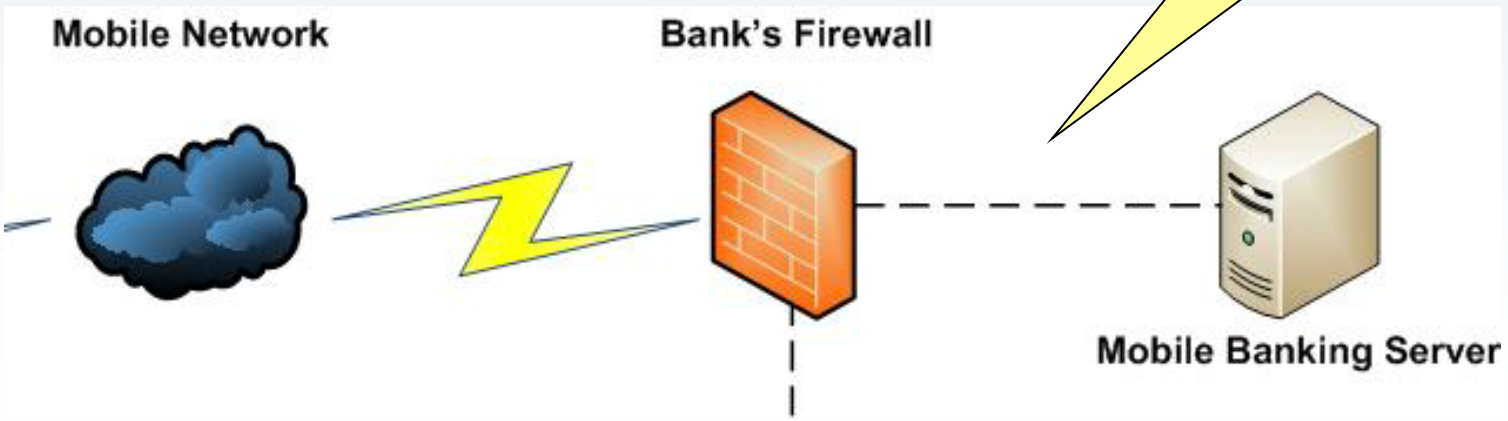
- Vulnerabilities and risks at each component
- Perform a risk assessment
  - Server Side Risks
  - (Vendor Risks)
  - Transmission Risks
  - Mobile Device Risks
  - Mobile App Risks
  - End User Risks

Risk Assessment Heat map



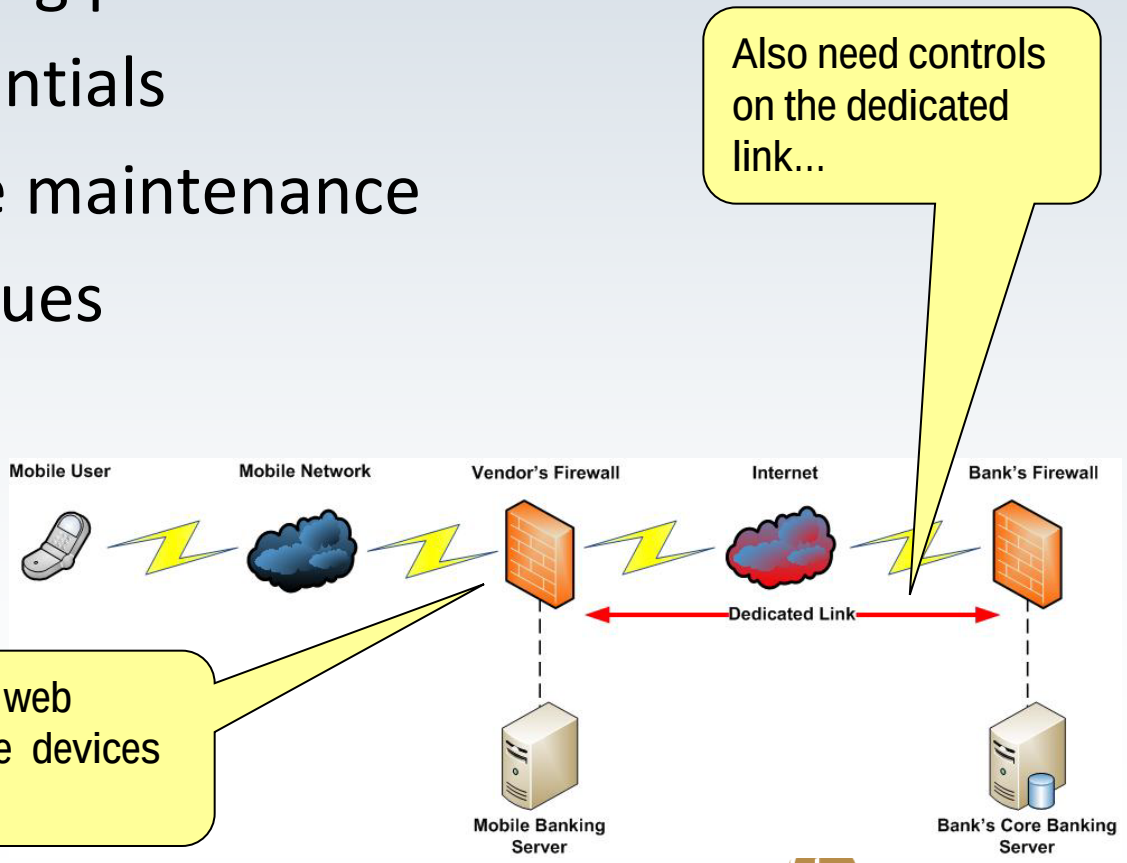
Vulnerabilities, Risks, & Controls

- Server Side Risks – Essentially the same as traditional Internet banking website risks
  - ◊ Insecure coding practices
  - ◊ Default credentials
  - ◊ Patch/update maintenance
  - ◊ Certificate issues



Vulnerabilities, Risks, & Controls

- Vendor Risks – Same risks as banks – now outside of your direct control.
  - ◊ Insecure coding practices
  - ◊ Default credentials
  - ◊ Patch/update maintenance
  - ◊ Certificate issues



Vulnerabilities, Risks, & Controls

- Transmission Risks
  - Most mobile devices have always on Internet connection
    - ◊ Cellular (cell phone service provider)
    - ◊ Wifi (802.11 – home, corporate, “public”)
  - Need encryption
  - Common end user practices

Vulnerabilities, Risks, & Controls

- Mobile Device Risks
  - Multiple hardware platforms & multiple operating systems

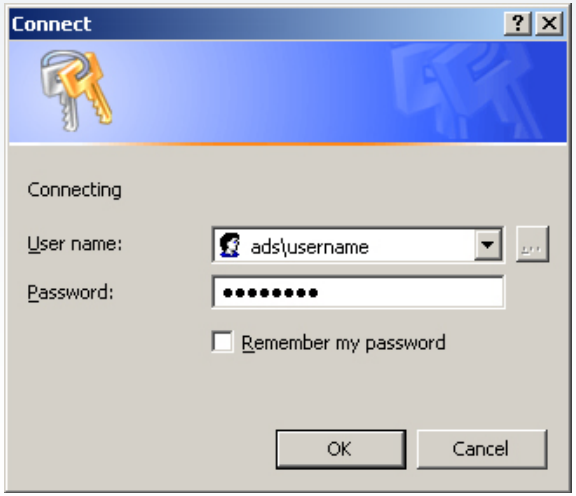
- Apple iOS
- Android
- BlackBerry
- Windows Mobile
- Symbian

Vulnerabilities, Risks, & Controls

- Mobile App Risks
  - Secure coding issues
  - Installation of App
  - Use and protection of credentials
  - Storage of data
  - Transmission of data

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">
    <head>
        <meta http-equiv="Content-Type" content=
        "text/html; charset=us-ascii" />
        <script type="text/javascript">
            function reDo() {top.location.reload();}
            if (navigator.appName == 'Netscape') {top.onresize = reDo;}
            dom=document.getElementById;
        </script>
    </head>
    <body>
    </body>
</html>
```



Vulnerabilities, Risks, & Controls

- End User Risks
  - Lose the device
  - Don’t use passwords, or use “easy to guess passwords”
  - Store passwords on the device
  - Jail break the device
  - Don’t use security software
  - Use/don’t recognize insecure wireless networks
  - Let their kids “use” the device

Compliance

- FFIEC Authentication Guidance
  - **More than just authentication**
  - Authentication
    - ◊ Same requirements as Internet banking
  - Monitoring and anomaly detection
  - Education

Compliance

- Authentication guidance references:

  "Although this guidance is focused on the risks and risk management techniques associated with the Internet delivery channel, **the principles are applicable to all forms of electronic banking activities**"

  "The agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions **involving access to customer information** or the movement of funds to other parties"

- http://www.ffiec.gov/pdf/authentication_guidance.pdf

Compliance

- Do not rely on single control
  - Controls need to increase as risk increases
  - Multi-layer
  - Additional controls at different points in transaction/interaction with customer
- Technical (IT/systems) controls

Compliance

- Customer awareness and education
  - Explanation of protections provided and not provided
  - How the bank may contact a customer on an unsolicited basis
  - A suggestion that commercial online banking customers perform assessment and controls evaluation periodically;
  - A listing of alternative risk control mechanisms that customers may consider implementing to mitigate their own risk
  - A listing of bank contacts for customer discretionary use to report suspected fraud

Vendor Due Diligence and Management

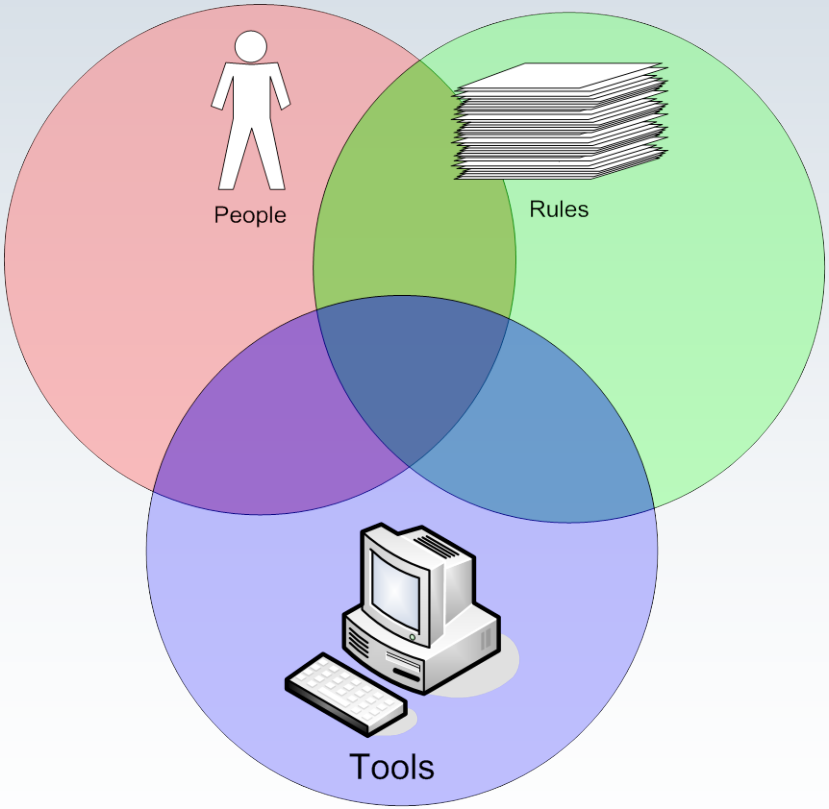
- All of the above – applies to your vendor(s)
  - Mobile banking application provider
  - Mobile banking hosting provider

- Contracts with SLA's
- SSAE16 reviews
- Independent code review and testing

Definition of a Secure System

"A secure system is one we can depend on to behave as we expect."

Source: "Web Security and Commerce" by Simson Garfinkel with Gene Spafford



- Confidentiality
- Integrity
- Availability

Questions?

Thank you!

Randy Romes, CISSP, CRISC, MCP, PCI-QSA
CliftonLarsonAllen, LLP
Information Security Services
Randy.Romes@cliftonlarsonallen.com
612-397-3114

References

- FFIEC Authentication Guidance
- http://ffiec.bankinfosecurity.com/
- http://www.ffiec.gov/pdf/pr080801.pdf (2001)
- http://www.ffiec.gov/pdf/authentication_guidance.pdf (2005)
- http://www.ffiec.gov/pdf/Auth-ITS-Final%206-22-11%20(FFIEC%20Formated).pdf (2011)
- Bank Info Security:
- http://ffiec.bankinfosecurity.com/
- FDIC ACH Advisories:
- http://www.fdic.gov/news/news/SpecialAlert/2011/index.html

References

Fraud Detection and Monitoring Solutions

- Guardian Analytics - FraudDesk
- http://www.guardiananalytics.com/products/FraudDESK/fraud-analyst.php
- Guardian Analytics - FraudMAP
- http://www.guardiananalytics.com/products/fraudMAP-overview/transaction-monitoring.php
- Easy Solutions – Detect Safe Browsing
- http://www.easysol.net/newweb/Products/Detect-Safe-Browsing
- Easy Solutions – Detect Monitoring Service
- http://www.easysol.net/newweb/Services/detect-monitoring-service
- Jack Henry Banking – Gladiator NetTeller ESM
- http://www.jackhenrybanking.com/products/risk/NetTellerESM
- ICT Solutions – Smart Fraud Monitoring
- https://sites.google.com/a/ictedu.info/ict-solutions/smart-application-suite/smart-fraud-monitoring

References

- SANS report
- http://www.sans.org/top-cyber-security-risks/summary.php

- Juniper Networks Malicious Mobile Threats Report:
- http://www.juniper.net/us/en/local/pdf/whitepapers/2000415-en.pdf

- Sybase Mobile Commerce Guide 2012:
- http://www.sybase.com/mobilecommerceguide

References

Juniper Networks Malicious Mobile Threats Report:

http://www.juniper.net/us/en/local/pdf/whitepapers/2000415-en.pdf

Safeguards of enterprises:

- On-device anti-malware
- On-device firewall
- Centralized remote locate, track, lock, wipe, backup and restore facilities for
- Centralized administration to enforce and report on security policies across the entire mobile device population
- SSL VPN clients to effortlessly protect data in transit, and to ensure secure and appropriate network access and authorization
- Device monitor and control, such as the monitoring of messaging and control of installed applications
- A solution that integrates with network-based technologies, such as network access control (NAC), to ensure the security
- posture of mobile devices and determine appropriate access rights prior to allowing access to corporate resources
- Management capabilities to enforce security policies, such as mandating the use of PINs/passcodes
- Ability for an administrator to monitor device activity for data leakage and inappropriate use

References

Juniper Networks Malicious Mobile Threats Report:

http://www.juniper.net/us/en/local/pdf/whitepapers/2000415-en.pdf

Safeguards of consumers:

- On-device anti-malware
- On-device personal firewall
- Password protection for device access
- Remote locate, track, lock, wipe, backup and restore software
- Antispam software to protect against unwanted voice and SMS/MMS communications

For parents - device usage monitoring software to monitor and control pre-adult mobile device usage and protect against

- cyberbullying, cyberstalking, inappropriate use, and other online threats, including automated alerting for:
- SMS message content
- Email message content
- Insight into pictures taken, sent, and received by the device, as well as those stored on the device
- Installed applications
- Address book and contact lists