Security and Privacy Issues on Current and Future Internet

Souhwan Jung

Soongsil University

souhwanj@ssu.ac.kr

Outline

- **Features of Current Internet**
- **Security and Privacy Issues on Current Internet**
- **Future Internet**
  - Challenges
  - Requirements
- **Security Issues on Future Internet Architectures**
- **Summary**

What is the Internet?

- **Collection of networks that communicate**
  - with a common set of standard protocols (TCP/IP)
  - by multilateral agreement
- **Collection of networks with**
  - no central control
  - no central authority
  - no common legal oversight or regulations
  - no standard acceptable use policy
- **Physical network connections are not important**
  - leased lines, dial-up, wireless
- **Logical connectivity**
  - everything is connected to everything else

Security Issues on Current Internet (1/2)

- **Internet Infrastructure is Inherently Insecure**
  - Security was not a design consideration of Internet protocols
  - Unauthenticated routing protocols control Internet reachability
  - Add-on security is hard on users and hard to integrate into applications

- **Vulnerable Software Everywhere**
  - Vulnerability in software is unavoidable and continues to appear
  - Vulnerable security products are already deployed

Security Issues on Current Internet (2/2)

- **Sophistication & Automation of Attack Tools**
  - Attack tools / toolkits are becoming more sophisticated, automated, easy to use & hard to trace back
  - No specific knowledge required to mount attacks
  - Global collaboration for attack is getting more common.

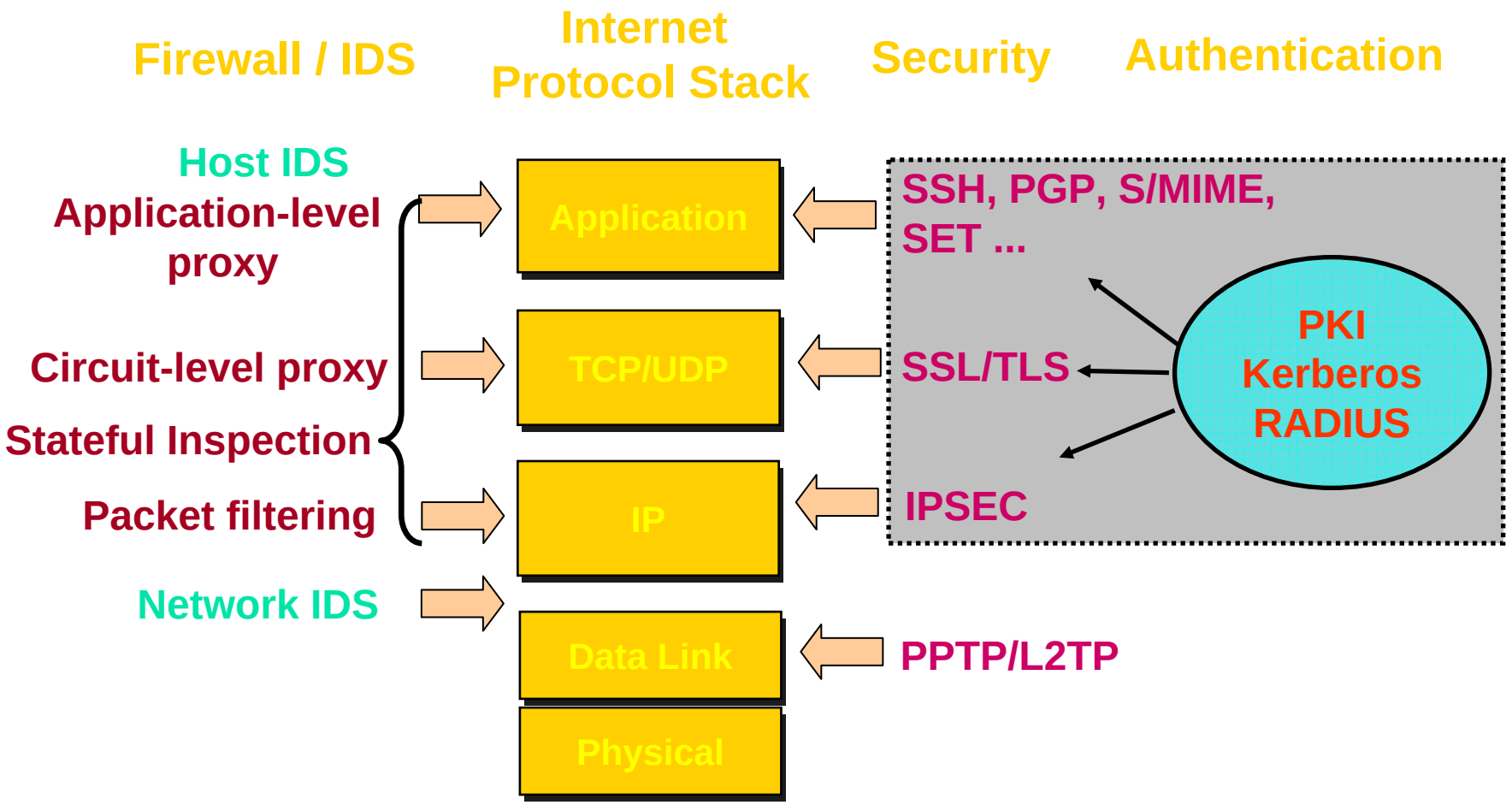
- **More Distributed Networking / Applications Emerging**
  - Distributed file sharing/computing
  - Peer-to-peer networking, home networking
  - Ubiquitous computing

Passive & Active Attacks

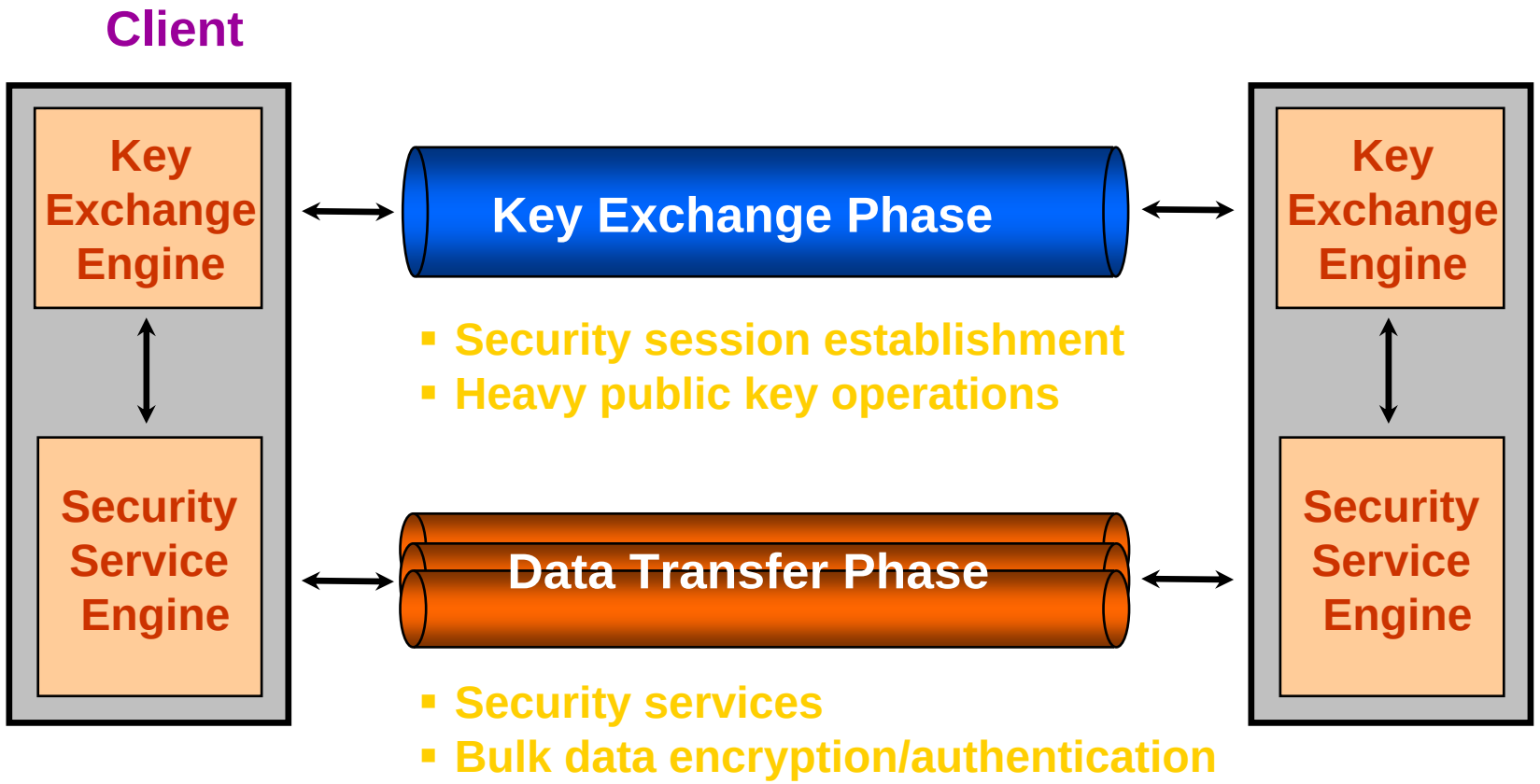
- **Passive**
  - Sniffing
  - Wiretap
  - TEMPEST : detecting information from Transient Electromagnetic Pulse
  - Social Engineering

- **Active (Program)**
  - Worm (independent) : program that replicates itself through network
  - Logic bomb : malicious instructions that trigger on some event in the future, such as a particular time setting
  - Trojan horse : program that does something unexpected (and often secretly)
  - Trapdoor : an undocumented entry point intentionally written into a program, often for debugging purposes, which can be exploited as a security flaw
  - Virus : program fragment that, when executed, attach itself to other programs

Security Solutions for Current Internet



Security Solutions for Networks



❖ Examples: IPSec, SSL/TLS/WTLS, SSH …

Status of Current Internet Security

- **Limitation on current security technology**
  - Separation of security function from network
    - Independent deployment of virus vaccine, spam filter, IDS, Firewall, VPN, etc, in each layer and application whenever necessary
  - Passive detection and prevention
    - Passive reaction by relying on the decision of human
    - Long delay until action, which allows additional attacks

- **More importantly, integrated end-to-end security measures are not available**
  - Local detection of worm, DDS and BoT
  - Each domain has its own security measures
  - No correlation among security technologies
  - No integrated end-to-end security measures

Contents

- **Introduction**
  - Current Internet
- **Security and Privacy Issues on Current Internet**
- **Future Internet**
  - Challenges
  - Requirements
- **Security Issues on Future Internet Architectures**
- **Conclusion**

What is the Future Internet?

- **Future Internet**
  - Clean Slate design of the Internet's architecture to satisfy the growing demands
  - Management issues of Future Internet also need to be considered from the stage of design

- **Research Goal for Future Internet**
  - Performing research for Future Internet and designing new network architectures
  - Building an experimental facility

Features of Future Internet Architecture

- **Virtualization**
  - Virtualizes network resources and provide customer-specific services
- **Service-Oriented Architecture (SOA)**
  - Define layer's functions as services and converge the services to support the network operations
  - Register services, discover services in repository and acquire necessary services
- **Cross-layer design**
  - Divide network layers and support a cross-layer mechanism

Why need the Future Internet Security?

- **Change of the security paradigm**

Current	Future
- Passive, Reactive - Single layer/Equipment - Detection Afterwards - Bolted-on service - Separation from network	- Automatic, Active - Multilayer integration - Detection in advance - Built-in service - Integration to network

Security is no more an option

Reference: Security research in Future Internet, Korea-EU ICT forum

Challenges for Security

- **Current Internet**
  - No explicit consideration on security
- **New security architectures, models and frameworks should address the emerging vulnerabilities and threats**

- **Challenges for security**
  - Managing and protecting the identity of billions of networked persons, devices, services and virtual entities connected in the Future Internet
  - Securing the interactions and interfaces from heterogeneous ICT (Information and Communication Technology) systems and engineering with scalable security policies across the Future Internet
  - Securing critical infrastructures that are interdependent and controlled through vulnerable networks
  - Security of highly distributed virtual entities and trusted infrastructures based on virtualized communication, computing and storage resources

Challenges for Privacy

- **Current Internet**
  - Leaving a life-long trail of personal data
- **In the Future Internet new tools and policies should be developed**
  - Provide user-centric identity management
  - Protect life-long privacy of users and their personal entities
- **Challenges for privacy**
  - Understanding and developing privacy-friendly identity management schemes
  - New frameworks and reference architectures integration
    - Fragmented approaches for managing personal information and for sharing data exchanged under user's control

Security Requirements (1/3)

- **Availability**
  - Should achieve a level of availability suitable
    - For “mission-critical” activities
    - For continued operation in times of crisis and attack
- **Dealing with the end-node**
  - Most vexing issues today
    - The poor state of end-node security
    - The implications for the overall security state of the network
    - End-node problems
      - Zombies, phishing, spam, spyware, and viruses
  - Future Internet Security should take a considered and defensible position on the role of the network in protecting and supporting the end-nodes
  - Proposed a consistent division of responsibility between the network, the end-node system, and the application

Security Requirements (2/3)

- **Usable security**
  - Good security makes a system hard to use
  - The most desirable security tools are those are not “best”
  - Creating mechanisms that are easy to use

- **Flexible outcomes**
  - Different contexts call for different degrees of security
    - A corporation, the government and an individual may have different needs and expectations
  - An architecture should not dictate one outcome
    - Should allow the level of security to be turned to the task at hand
    - Should try to give that control to the end-users as possible

Security Requirements (3/3)

- **Coherent design**
  - How the various security mechanisms fit together to provide a consistent and coherent security outcome
  - This requirement is not a call for a uniform security outcome
- **Security for tomorrow's devices**
  - Today's Internet is populated by work stations and server, and smaller devices such as PDAs
  - Tomorrow's world will be populated by even smaller devices, embedded processors and sensors

Contents

- **Introduction**
  - Current Internet
- **Security and Privacy Issues on Current Internet**
- **Future Internet**
  - Challenges
  - Requirements
- **Security Issues on Future Internet Architectures**
- **Conclusion**

Security Issues on Future Internet Architectures

- **No successful solutions**
- **Trade-offs**
  - Between usability and security
  - Between identity and privacy
- **Models for Future Security Architectures**
  - Network centric security architectures
  - Host centric security architectures
- **Trends of Future Internet**

Models for Future Security Architectures (1/2)

- **Network centric security architectures**
  - Advantages of perimeter-based security models
    - They focus on site security definition, management, enforcement and auditing at a very limited number of points in the network
    - Perimeter security points are under the total control of enterprise security organizations
    - The most highly maintained and monitored assets in enterprise network infrastructures

Models for Future Security Architectures (2/2)

- **Host centric security architectures**
  - Traditional perimeter models are becoming obsolete
    - Because the growing impotence and acceptance
      - Nomadic devices, self organizing systems (e.g., Ad hoc), environments with untrusted local links (e.g., public wireless access points)
  - But, host centric security architecture is immature
  - Possibility of host centric security architecture with the use of IPv6
    - Better suited to enable such host centric security models
      - IPv6 is provision of globally unique and routable address
      - Mandatory support of IPSec in all implementations

Trends of Future Internet

- **US**
  - FIND (Future Internet Design) December 2005
  - GENI (Global Environment for Network Innovation) August 2005
- **Europe**
  - FIRE (Future Internet Research and Experimentation Activities), 2007
- **KOREA**
  - Future Internet Forum, 2006

US - FIND

- **What is FIND?**
  - Major new long-term initiative of NSF NeTS research program
  - Funded project seeking to design a next-generation Internet called the 'Future Internet'

- **Security goal of FIND**
  - A Future network must offer greatly improved security and robustness

- **Security Issues**
  - How can we design a network that is fundamentally more secure and available than today's Internet?
  - How would we conceive the security problem if we could start from scratch?
  - How do we protect the control traffic?
    - Ensure only authorized users can configure
  - How should the network protect against DoS?

US - GENI

- **What is GENI?**
  - A planning effort initiated by the NSF CISE Directorate
  - Experimental facility to validate research (infrastructure to demonstrate research)
  - A nationwide programmable facility for research into Future Internet technologies

- **Security Goal**
  - GENI should be secure, so that its resources cannot accidently or maliciously be used to attacking today's Internet
    - To use technical and operational means to prevent, detect, and manage attacks
    - To render the GENI system to be both safe and usable

Security Issues

- **Security Issues**
  - How security should be architected into globally distributed systems of networks and computers?
  - How to design the access control framework?
    - E.g., Authentication and authorization architecture
  - How the end users protect against DoS?
  - GENI is needed to ascertain the circumstances
    - Privacy policies would impose on the efficiency or the possibility of completing access proofs

UE – FIRE

- **What is FIRE?**
  - An activity or initiative aims to scope and consolidate the European work in networking testbeds

- **Goal**
  - Aims at providing a research environment for investigating and experimentally validating highly innovative and revolutionary ideas on future Internet

Security and Privacy Issues in FIRE

- **Security Issues**
  - How to protect the Future Internet and Current Internet's against emerging threats?
  - How to protect the end-users and their devices?
  - Self-protected and resilient networks and service platforms?
  - How to measure and assess the security of Future Systems?

- **Privacy Issues**
  - How to deal with "identities" of billions of entities?
  - Who is going to be a manage for the ID?
    - User or Big brother
  - How to protect our personal sphere?
    - User centricity or Big brother

Korea - FIF

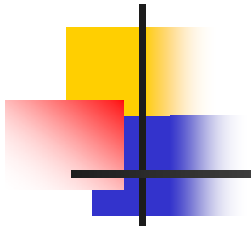
- **Future Internet Forum (FIF)**

- **First forum meeting –September, 2006**
  - First stage: to June, 2007
    - Review prior activities related to future Internet research
  - Second stage
    - Propose areas that we can contribute most
    - Problem definition

- **Topics**
  - Naming, routing
  - Large-capacity switching
  - Wireless networking
  - LBS & context-aware services

Summary

- **Change of the security paradigm**
  - Security is no more an option
- **Existing various challenges**
  - For security
  - For privacy
- **Existing various security requirements**
  - Availability, Dealing with the end-node, Usable security, Flexible outcomes, Coherent design, and Security for tomorrow’s devices
- **But, No successful solutions so far!**



Thank you!