

Wireless Network Security as We See It: State of Affairs and the Road Ahead

NSF Wireless Security Workshop

April 11, 2008

Alex Reznik, CTO Office, InterDigital



Outline

- The Big Picture:
 - From secure data comm. to secure wireless networks
 - Trying to put it together – which pieces are needed
- PHY-layer security at InterDigital
 - The theory (pieces of the puzzles)
 - Enabling PHY-layer security on modern systems
- Looking forward: the challenges



The Big Picture

April 11, 2008



Modern Wireless Networks and Security

- Design principles based upon the wired network
 - Physical layer is inherently secure, point-to-point, authenticated and available
- Little emphasis on the security/robustness of the network
 - Security
 - Primarily peer-to-peer
 - Rudimentary at Access Level and dependent on higher layer components
 - Platform security
 - Link quality/robustness
 - Managed primarily by MAC layer and above procedures
 - Minimal use of PHY-layer information
- Prevailing “IT world” philosophy
 - Security
 - Data is key. We need to be able to
 - Secure it against eavesdropping
 - Control and restrict access to it
 - The NETWORK is just there to move it
 - Result: protect data, NOT the network
 - Wireless access viewed as a derivative of a wired network
 - Access component is just another plug-in



Is This OK for Wireless? – We Think NOT

- Wireless networks are inherently vulnerable in a way that wired networks are not
 - Network violation does not require physical access to protected facilities
 - Network can be brought down with ease
 - Unauthenticated access possible (just start sending)
 - Information is of a broadcast nature and extends beyond physical boundaries
 - Sources are not authenticated (can be spoofed at the MAC/PHY level)
- This is a general problem
 - Security is usually only as good as the complete system
 - While app. data may remain secure, network *availability* remains a vulnerability
 - Remotely placed nodes and terminals may be easily modified and compromised
 - Scarce resources used for data pipes in wireless systems have been oversized to provide for reliable QoS and data availability
- In particular, this is a problem for wireless networks with little above the Access Level
 - Sensors and monitoring
 - Control applications

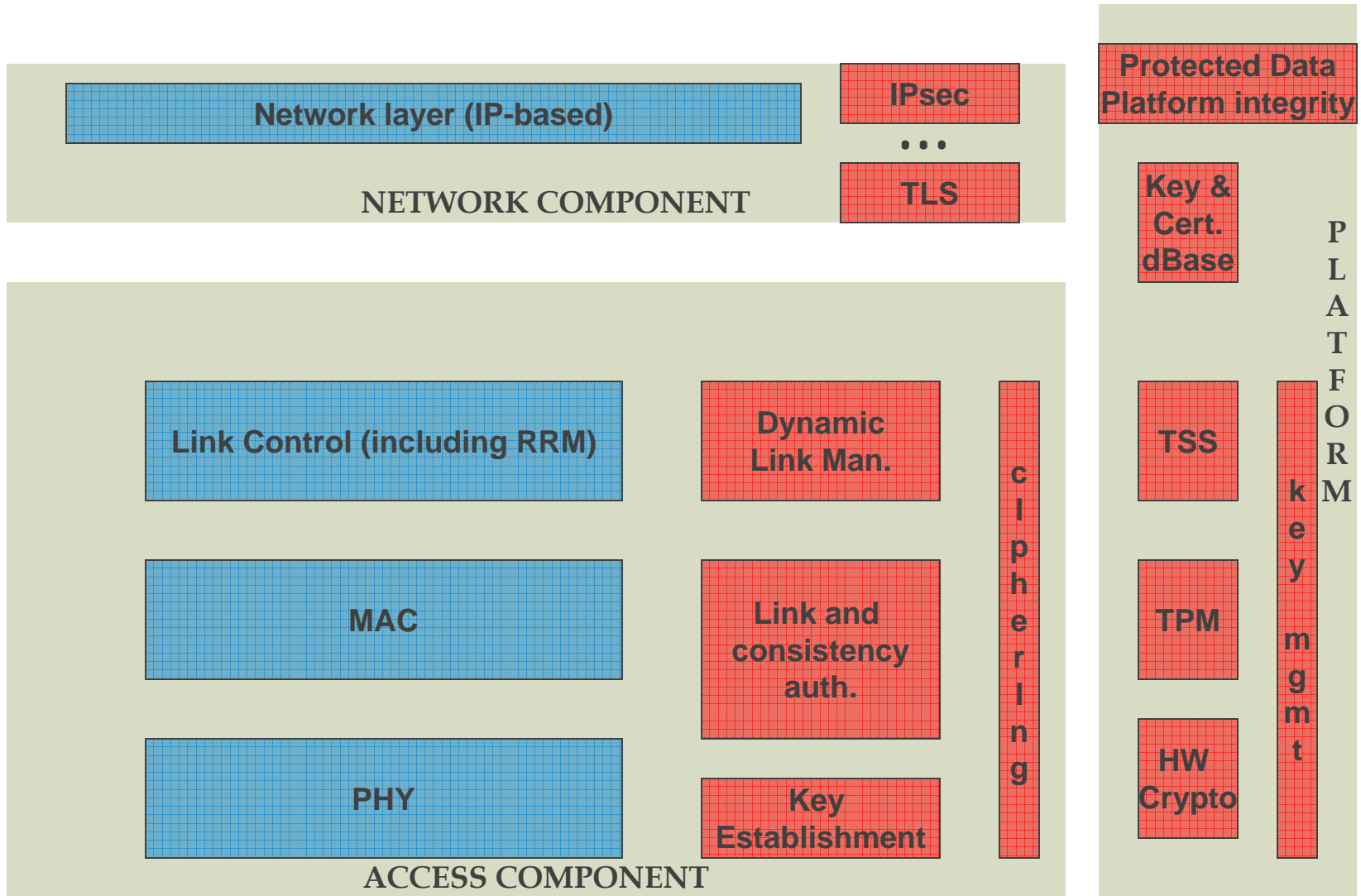


What Can be Done ?

- Continual improvements in data and user security needed
 - Common with wired network security
 - Address the needs at the higher layers which are transport agnostic
- Secure the wireless link
 - This is what is commonly known as “PHY-layer security,” although it often involves PHY, MAC and aspects of higher layers
 - Simplistically, the goal is to achieve the security attributes of a wire:
 - Availability
 - Anti-spoofing/jamming
 - Anti-eavesdropping
 - Additionally, physical medium is exploited to enhance overall security
- Secure the platform
 - Prevent false user authentication from taking place on your platform?
 - Can your encrypted packets be secretly decrypted and siphoned off?
 - Can the keys for your encrypted data be securely stored and handled?
- How do we put it all together?
 - Not really clear, but we can try an ad-hoc approach

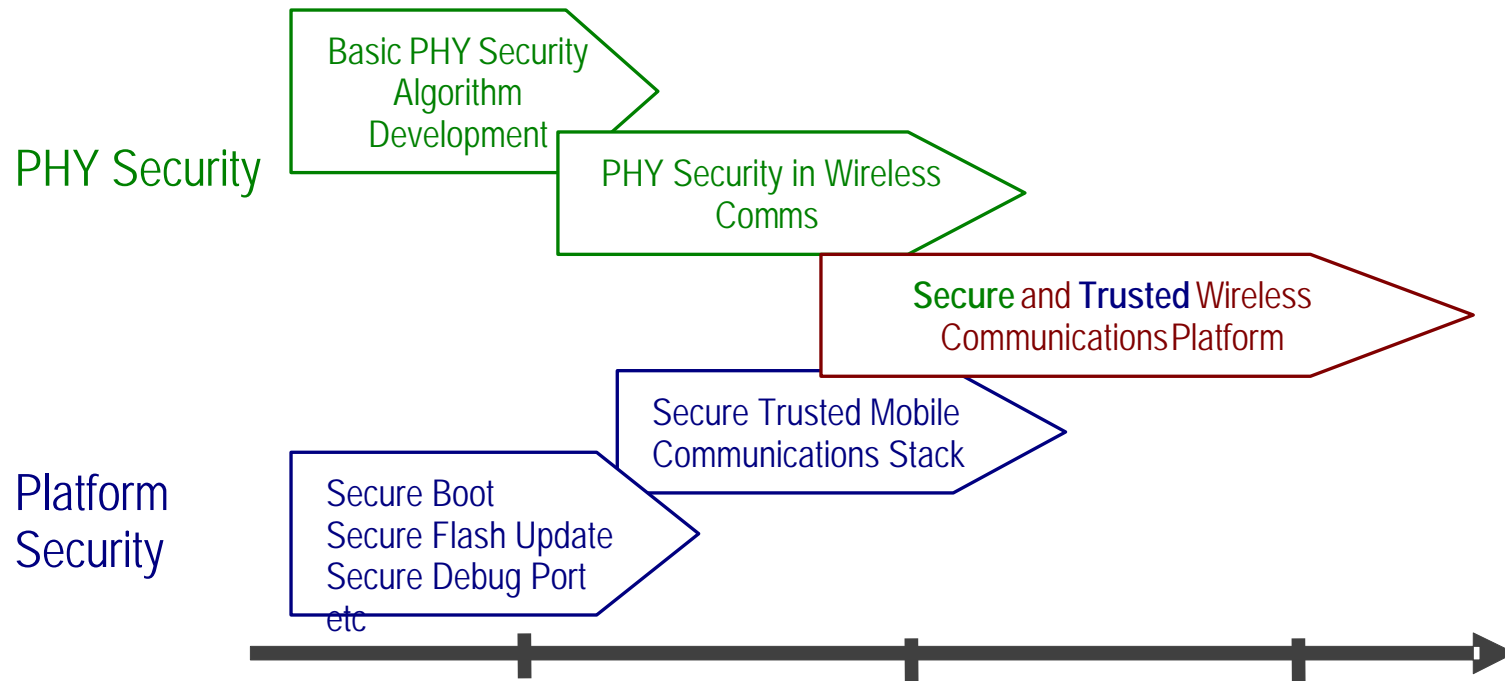


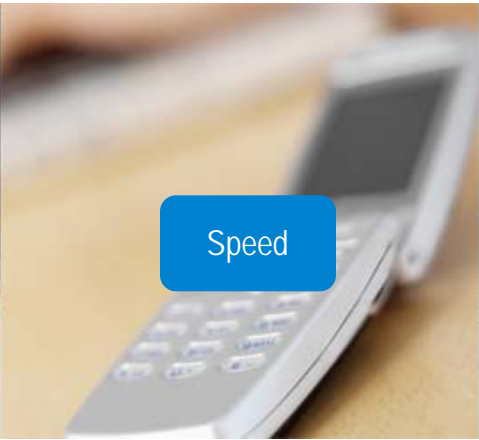
Example: Control and Monitoring Systems with Security





InterDigital Security Roadmap





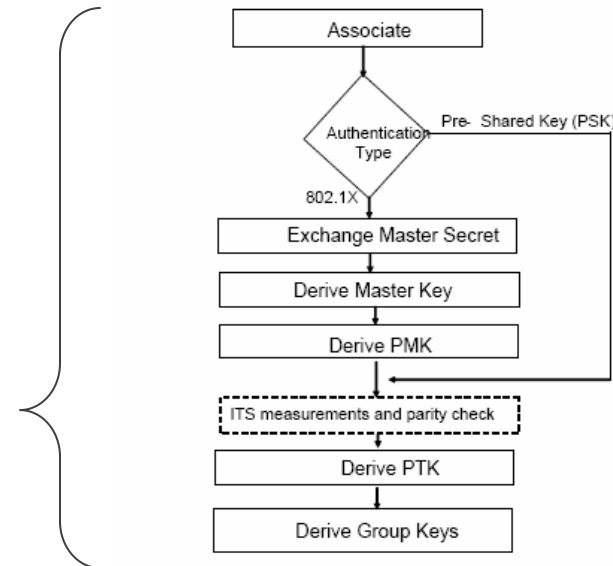
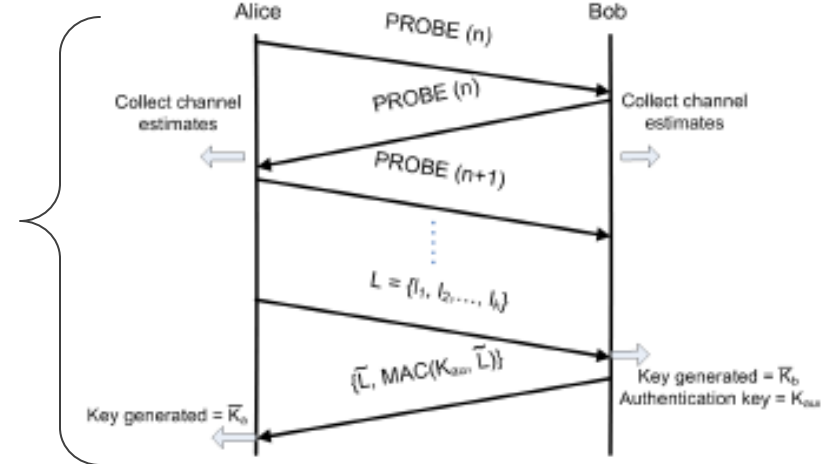
PHY-Layer Security

April 11, 2008



What is InterDigital Doing

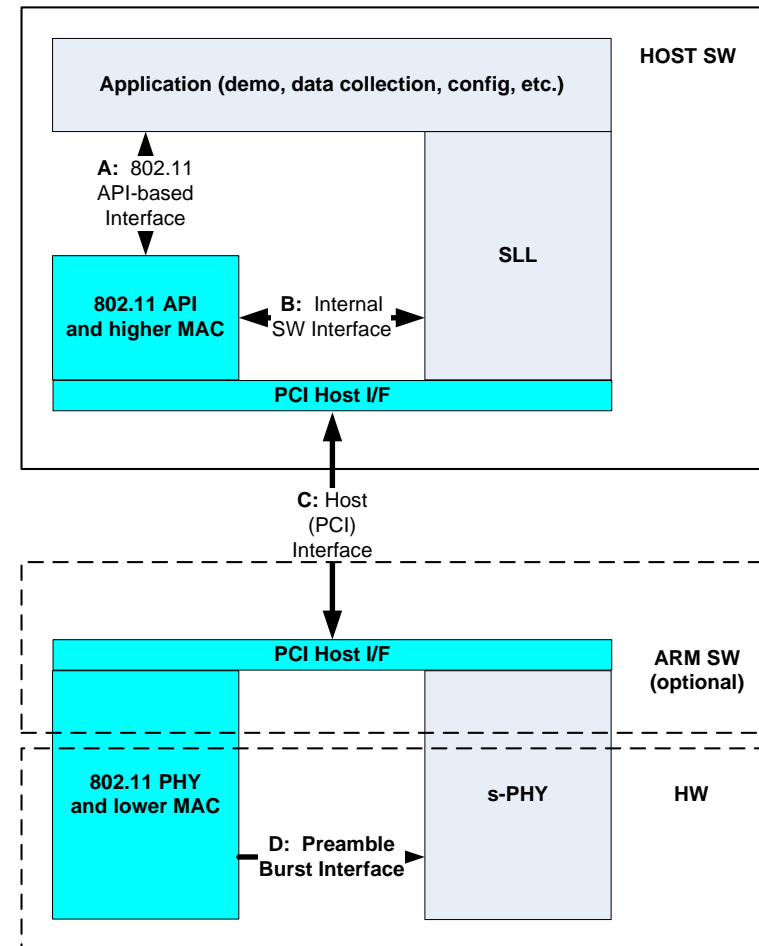
- Information theoretic secret-key generation
 - Collaborative effort between Rutgers and InterDigital
 - On the platform Summer 2008
- Authenticated communications through PHY-Security
 - Developed at Rutgers
 - Joint implementation on platform starting Q2 2008
- Integration towards a "complete solution" mid-late 2009
 - Extensions to enhanced 802.11i security ~Q1 2009
 - Full "low-layer" security manager in 2009
 - Targeting standards, e.g. IEEE and ISA





Architecting a PHY-Security Platform

- Targeted to support a comprehensive wireless security system
 - Compliment existing security layers
 - Strengthen overall system security through introduction of PHY-Security layer
- Develop and test attack scenarios
- 802.11-based but applicable to many wireless standards





The Challenges Ahead

- Secure Wireless Systems
 - Clearly neither “IT security” to “PHY-layer security” are sufficient
 - What does a completely secure wireless system look like?
 - The role of economics
- Enabling “PHY-security” technology
 - Formal security models
 - Taking existing theory to practice
 - Enabling measurements and signal processing support
 - Standardization as appropriate
- Education and evangelization
 - Security typically viewed as a non-PHY problem
 - “PHY-layer” security not accepted
 - IT community – “its a PHY issue”
 - Comms community – “it’s a security issue”
 - Need to educate the community that the two world have not converged



Thank You

Alex.Reznik@InterDigital.com

April 11, 2008