

Track 17: The New Attacker Model



Dr. Ghassan Karame

NEC Laboratories Europe
Heidelberg, Germany

ghassan@karame.org

www.ghassankarame.com

The Surge of a New Attacker Model



"We know you're upset, we hear you.
Believe me, we're listening. We read you.
You're coming in loud and clear."

Image Source: TheLaw.tv



Image Source: pcworld.com

The Surge of a New Attacker Model

Global surveillance [\[edit\]](#)

Main article: Global surveillance

Global surveillance programs		
Program	International contributors and/or partners	Commercial partners
 PRISM	<ul style="list-style-type: none">  Australian Signals Directorate (ASD/DSD) of Australia^[49]  Government Communications Headquarters (GCHQ) of the UK^[50]  Algemene Inlichtingen en Veiligheidsdienst (AIVD) of the Netherlands^[51] 	<ul style="list-style-type: none"> Microsoft^{[33][52][53]}
 XKeyscore	<ul style="list-style-type: none">  Bundesnachrichtendienst (BND) of Germany^{[6][54]}  Bundesamt für Verfassungsschutz (BfV) of Germany^{[6][54]}  National Defence Radio Establishment (FRA) of Sweden^{[55][56]} 	
 Tempora	<ul style="list-style-type: none">  National Security Agency (NSA)^{[57][58]} 	<ul style="list-style-type: none"> British Telecommunications (codenamed "Remedy")^[59] Interoute (codenamed "Streetcar")^[59] Level 3 (codenamed "Little")^[59] Global Crossing (codenamed "Pinnacle")^[59] Verizon Business (codenamed "Dacron")^[59] Viatel (codenamed "Vitreous")^[59] Vodafone Cable (codenamed "Gerontic")^[59]
 Muscular	<ul style="list-style-type: none">  NSA^[60] 	
 Project 6	<ul style="list-style-type: none">  Central Intelligence Agency (CIA)^[61] 	
Stateroom	<ul style="list-style-type: none">  DSD^{[62][63]}  Communications Security Establishment Canada (CSEC)^{[63][64]}  GCHQ^{[63][65]}  Special Collection Service (SCS)^{[63][65][66]} 	Source: wikipedia
Lustre	<ul style="list-style-type: none">  NSA^{[67][68]}  Direction Générale de la Sécurité Extérieure (DGSE) of France^{[67][68]} 	

Last updated: December 2013

The *New Attacker*

The new attacker controls the entire network

- Mining data from social networks and Internet Service Providers (ISPs)
- Performing illegal digital taps on private communication channels between individuals.

The new attacker controls the secret keys

- Secret keys were acquired by means of coercion, backdoors, etc.



Image Source: ixdaily.com

This panel

This panel will explore possible avenues to enhance user privacy in the presence of a powerful attacker model.



Empowered by Innovation

NEC