GUÍA DOCENTE
CURSO 2015-16

FICHA TÉCNICA DE LA ASIGNATURA

Datos de la asignatura	
Nombre	Seguridad en Sistemas de Comunicación
Código	DTC-TEL-612
Titulación	Máster en Ingeniería de Telecomunicación
Curso	Segundo
Cuatrimestre	1º
Créditos ECTS	4,5
Carácter	Obligatorio
Departamento	Telemática y Computación
Área	Seguridad Informática
Coordinador	Ángel Prado

Datos del profesorado	
Profesor	
Nombre	Ángel Prado
Departamento	Telemática y Computación
Área	Seguridad Informática
Despacho	
e-mail	
Teléfono	
Horario de Tutorías	Contactar por email para pedir cita

Datos del profesorado	
Profesor	
Nombre	Rafael Palacios
Departamento	Telemática y Computación
Área	Seguridad Informática
Despacho	Planta 5. Dirección
e-mail	Rafael.Palacios@iit.comillas.edu
Teléfono	
Horario de Tutorías	Contactar por email para pedir cita

DATOS ESPECÍFICOS DE LA ASIGNATURA

Contextualización de la asignatura

Aportación al perfil profesional de la titulación

En el perfil profesional del Ingeniero de Telecomunicación, esta asignatura proporciona un conocimiento de los conceptos y principios de gestión de la seguridad informática y de las comunicaciones.

Al finalizar el curso los alumnos deben conocer las herramientas necesarias para la gestión y gobierno de la seguridad tanto a nivel de comunicaciones como de infraestructura informática. Los alumnos deben estar familiarizados con las técnicas de ataque y las tecnologías de protección, monitorización y análisis de la seguridad.

La asignatura tiene un carácter mixto teórico-experimental por lo que a los componentes teóricos se les añaden los de carácter práctico, realizando trabajos y pruebas dentro del ambiente controlado del laboratorio de comunicaciones del ICAI.

Prerrequisitos

Conocimientos generales sobre redes de comunicaciones (LAN).
Conocimientos generales sobre arquitecturas TCP-IP.
Conocimientos generales sobre protocolos de seguridad y VPN.

BLOQUES TEMÁTICOS Y CONTENIDOS

Contenidos – Bloques Temáticos

Capítulo 1: Introducción y visión general

1.1 Ciberseguridad en 2015
1.2 Brechas de seguridad destacables
1.3 Cómo es el día del personal de seguridad

Capítulo 2: Fundamentos de http y de los navegadores

2.1 Anatomía de Internet
2.2 Peticiones y respuestas en HTTP
2.3 Sesiones y cookies
2.4 Características de seguridad del navegador
2.5 Políticas de origen común
2.6 Codificación de entidad y JavaScript
2.7 Características nuevas de HTML5
2.8 Peticiones entre dominios (cross-domain)
2.9 Mensajes POST y almacenamiento local
2.10 Identificación del navegador (Fingerprinting)

Capítulo 3: Modelo de amenaza y pruebas de penetración

3.1 Modelado de vectores de ataque
3.2 Amenazas y estrategias de defensa
3.3 Revisión de código y análisis de tráfico

3.4 Ciclo de vida de desarrollo seguro 3.5 El modelo STRIDE
Capítulo 4: Ataques contra la capa de aplicación
4.1 Referencias inseguras a objetos 4.2 Configuraciones inseguras 4.3 Autenticación vulnerable 4.4 Gestión de sesión vulnerable 4.5 Autorización vulnerable 4.6 Ataques RTL (Right to Left) 4.7 Ataques con CAPTCHA 4.8 Aprovechamiento de los Metadatos públicos 4.9 Contraseñas débiles 4.10 Redirección de DNS
Capítulo 5: Vulnerabilidad web habituales
5.1 OWASP top 10 5.2 Cross-Site Scripting (XSS) 5.3 Cross-Site Remote Forgery (CSRF) 5.4 Ataques de XML external entity 5.5 Robo de clicks (Clickjacking) 5.6 Redirecciones abiertas 5.7 Inyección SQL 5.8 Inyección SQL ciega 5.9 Denegación de servicio 5.10 Ataques Mutation XSS (mXSS) 5.11 Ejecución de origen común
Capítulo 6: Ataques contra SSL
6.1 SSL stripping 6.2 Mezcla de contenidos HTTPS y HTTP 6.3 Cómo evitar la seguridad de transporte HSTS 6.4 BREACH 6.5 LUCKY 13 6.6 RC4 biases 6.7 POODLE 6.8 Heartbleed
Capítulo 7: Ataques avanzados de canal lateral (side-channel)
7.1 BEAST 7.2 Ataques por hora y caché 7.3 Ataques haciendo uso de Unicode 7.4 Inspección de contenido y políglotas 7.5 Rosetta Flash 7.6 SMB relay 7.7 Estimar la localización (geoinference)

Capítulo 8: Seguridad en aplicaciones móviles
8.1 El modelo de las sandbox 8.2 Visión global de la seguridad en Android 8.3 Visión global de la seguridad en iOS 8.4 Gestión de dispositivos móviles (Mobile Device Management MDM) 8.5 Comprobación de aplicaciones móviles 8.6 Pinning de certificados
Capítulo 9: Sistemas de gestión de la seguridad
9.1 Estándares de gestión 9.2 Políticas de seguridad 9.3 Controles de seguridad 9.4 Acceso a la red 9.5 Gestión de identidades 9.6 Valoración del riesgo
Capítulo 10: Vigilancia de la seguridad y análisis forense
10.1 Sistemas de prevención y de detección de intrusiones 10.2 Cortafuegos de red 10.3 Análisis forense 10.4 Detección de anomalías 10.5 Respuesta a incidencias 10.6 Gestión de crisis 10.7 Amenazas Persistentes Avanzadas (APT)
Capítulo 11: Políticas y gobierno de la seguridad
11.1 Integridad del negocio 11.2 Gestión de la privacidad 11.3 Prevención del fraude 11.4 Gestión de las amenazas y vulnerabilidades 11.5 Planes de continuidad de negocio 11.6 Políticas de seguridad de la información empresarial
Capítulo 12: Confianza y cumplimiento de la legislación
12.1 Introducción a la certificación y los estándares 12.2 PCI DSS , FISMA, GLBA, SOX, ISO 27001 and HIPAA 12.3 Ley de protección de datos de España (LOPD) 12.4 Iniciativas comunes de seguridad en la Unión Europea 12.5 Residencia de los datos y cuestiones de privacidad de la información

Competencias – Resultados de Aprendizaje
Competencias
Competencias Generales
CG2. Capacidad para la dirección de obras e instalaciones de sistemas de telecomunicación, cumpliendo la normativa vigente, asegurando la calidad del servicio. CG3. Capacidad para dirigir, planificar y supervisar equipos multidisciplinares. CG7. Capacidad para la puesta en marcha, dirección y gestión de procesos de fabricación de equipos electrónicos y de telecomunicaciones, con garantía de la seguridad para las personas y bienes, la calidad final de los productos y su homologación. CG9. Capacidad para comprender la responsabilidad ética y la deontología profesional de la actividad de la profesión de Ingeniero de Telecomunicación.
Competencias de Formación Básica
CB3. Saber evaluar y seleccionar la teoría científica adecuada y la metodología precisa de sus campos de estudio para formular juicios a partir de información incompleta o limitada incluyendo, cuando sea preciso y pertinente, una reflexión sobre la responsabilidad social o ética ligada a la solución que se proponga en cada caso. CB4. Ser capaces de predecir y controlar la evolución de situaciones complejas mediante el desarrollo de nuevas e innovadoras metodologías de trabajo adaptadas al ámbito científico/investigador, tecnológico o profesional concreto, en general multidisciplinar, en el que se desarrolle su actividad. CB5. Saber transmitir de un modo claro y sin ambigüedades a un público especializado o no, resultados procedentes de la investigación científica y tecnológica o del ámbito de la innovación más avanzada, así como los fundamentos más relevantes sobre los que se sustentan.
Competencias del módulo de Tecnologías de Telecomunicación
CTT7. Capacidad para realizar la planificación, toma de decisiones y empaquetamiento de redes, servicios y aplicaciones considerando la calidad de servicio, los costes directos y de operación, el plan de implantación, supervisión, los procedimientos de seguridad, el escalado y el mantenimiento, así como gestionar y asegurar la calidad en el proceso de desarrollo.
Competencias de Gestión Tecnológica de Proyectos de Telecomunicación
CGT2. Capacidad para la elaboración, dirección, coordinación, y gestión técnica y económica de proyectos sobre: sistemas, redes, infraestructuras y servicios de telecomunicación, incluyendo la supervisión y coordinación de los proyectos parciales de su obra aneja; infraestructuras comunes de telecomunicación en

edificios o núcleos residenciales, incluyendo los proyectos sobre hogar digital; infraestructuras de telecomunicación en transporte y medio ambiente; con sus correspondientes instalaciones de suministro de energía y evaluación de las emisiones electromagnéticas y compatibilidad electromagnética.

Resultados de Aprendizaje

Al final de curso los alumnos deben ser capaces de:

RA1. Conocer las tecnologías de los sistemas de gestión de la seguridad de la información.

RA2. Conocer las estrategias, políticas y tecnologías de gobierno de la seguridad y saber aplicarlas en el diseño de una política segura de comunicaciones.

RA3. Conocer las certificaciones y estándares actuales de la seguridad así como las entidades internacionales de acreditación de la seguridad.

METODOLOGÍA DOCENTE

Aspectos metodológicos generales de la asignatura

Metodología Presencial: Actividades	Competencias
Clase magistral y presentaciones generales (25 horas presenciales). Exposición de los principales conceptos y procedimientos mediante la explicación por parte del profesor. Incluirá presentaciones dinámicas, pequeños ejemplos prácticos y la participación reglada o espontánea de los estudiantes.	**CG2, CG3, CG7, CG9 CB3, CB4, CTT7**
Resolución en clase de problemas prácticos (5 horas presenciales). Resolución de unos primeros problemas para situar al alumno en contexto. La resolución correrá a cargo del profesor y los alumnos de forma cooperativa.	**CB5**
Resolución grupal de problemas (5 horas presenciales). El profesor planteará pequeños problemas que los alumnos resolverán en pequeños grupos en clase y cuya solución discutirán con el resto de grupos.	**CB5, CTT7**
Prácticas de laboratorio (10 horas presenciales). Cada alumno realizará de forma aislada o en grupo una serie de prácticas de laboratorio regladas. Las prácticas de laboratorio finalizarán con la redacción de un informe de laboratorio o la inclusión de las distintas experiencias en un cuaderno de laboratorio.	**CB5, CGT2**

Metodología No presencial: Actividades	Competencias
El objetivo principal del trabajo no presencial es llegar a entender y comprender los conceptos teóricos de la asignatura, así como ser capaz de poner en práctica estos conocimientos para resolver los diferentes tipos de problemas.	
Estudio individual del material (45 horas no presenciales). Actividad realizada individualmente por el estudiante cuando analiza, busca e interioriza la información que aporta la materia y que será discutida con sus compañeros y el profesor en clases posteriores.	**CG9, CB3, CTT7, CGT2**
Resolución de problemas prácticos a resolver fuera del horario de clase por parte del alumno (20 horas no presenciales). El alumno debe utilizar e interiorizar los conocimientos aportados en la materia. La corrección a la clase se realizará por parte de alguno de los alumnos o el profesor según los casos. La corrección individualizada de cada ejercicio la realizará el propio alumno u otro compañero según los casos (método de intercambio).	**CB5, CGT2**
Trabajos de carácter práctico individual (25 horas no presenciales). Actividades de aprendizaje que se realizarán de forma individual fuera del horario lectivo, que requerirán algún tipo de investigación o la lectura de distintos textos.	**CB5, CGT2**

	ACTIVIDAD PRESENCIAL				ACTIVIDAD NO PRESENCIAL				RESULTADOS DE APRENDIZAJE	
Semana	h/sem	Clase teoría	Laboratorio	Evaluación	h/sem	Estudio individual	Problemas	Informes	RA	Descripción
1	2	Capítulo 1			1				RA2	Conocer las estrategias, políticas y tecnologías de gobierno de la seguridad y saber aplicarlas en el diseño de una política segura de comunicaciones
	1	Capítulo 2	Prácticas en clase		1				RA1	Conocer las tecnologías de los sistemas de gestión de la seguridad de la información
2	1	Capítulo 2	Prácticas en clase	Trabajo en clase	4					
	2	Capítulo 3			1				RA1	Conocer las tecnologías de los sistemas de gestión de la seguridad de la información
3	3	Capítulo 4	Prácticas en clase		9	Programas para casa			RA1	Conocer las tecnologías de los sistemas de gestión de la seguridad de la información.
4	2	Capítulo 4	Prácticas en clase	Trabajo en clase	4					
	1	Capítulo 5			1				RA1 y RA2	Conocer las tecnologías de los sistemas de gestión de la seguridad de la información. Conocer las estrategias, políticas y tecnologías de gobierno de la seguridad y saber aplicarlas en el diseño de una política segura de comunicaciones.
5	3	Capítulo 5	Prácticas en clase	Evaluación de problemas	9		Problemas	código		
6	3	Capítulo 5	Prácticas en clase	Trabajo en clase	3					
7	3	Capítulo 6			9	Lectura previa			RA1	Conocer las tecnologías de los sistemas de gestión de la seguridad de la información
8	3	Capítulo 6	Prácticas SSL		9	Prácticas SSL		Informe prácticas		
9	3	Capítulo 7	Prácticas en clase	Trabajo en clase	6				RA1	Conocer las tecnologías de los sistemas de gestión de la seguridad de la información
10	3	Capítulo 8		Presentación en clase	9	Lectura previa			RA1 y RA2	Conocer las tecnologías de los sistemas de gestión de la seguridad de la información. Conocer las estrategias, políticas y tecnologías de gobierno de la seguridad y saber aplicarlas en el diseño de una política segura de comunicaciones.
11	3	Capítulo 8			3					
12	3	Capítulo 9		Examen en clase	9	Estudio tema 9			RA2 y RA3	Conocer las estrategias, políticas y tecnologías de gobierno de la seguridad y saber aplicarlas en el diseño de una política segura de comunicaciones.
13	3	Capítulo 10			6	Lectura y Estudio de la teoría			RA1 y RA2	Conocer las tecnologías de los sistemas de gestión de la seguridad de la información. Conocer las estrategias, políticas y tecnologías de gobierno de la seguridad y saber aplicarlas en el diseño de una política segura de comunicaciones.
14	3	Capítulo 11			3				RA2	Conocer las estrategias, políticas y tecnologías de gobierno de la seguridad y saber aplicarlas en el diseño de una política segura de comunicaciones. Conocer las certificaciones y estándares actuales de la seguridad así como las entidades internacionales de acreditación de la seguridad.
15	3	Capítulo 12			3				RA3	Conocer las certificaciones y estándares actuales de la seguridad así como las entidades internacionales de acreditación de la seguridad.
	45				90					

EVALUACIÓN Y CRITERIOS DE CALIFICACIÓN

Actividades de evaluación	Criterios de evaluación	PESO
Realización de exámenes: • Examen Final (50%) • Pruebas intermedias (20%)	- Comprensión de conceptos. - Aplicación de conceptos a la resolución de problemas prácticos. - Tener en cuenta todos los aspectos críticos de seguridad. - Presentación y comunicación escrita.	**70%**
Evaluación del Rendimiento. • Prácticas: Trabajos de carácter práctico individual (30 %). •	- Comprensión de conceptos. - Aplicación de conceptos a la resolución de problemas prácticos. - Tener en cuenta todos los aspectos críticos de seguridad.	**30%**

Criterios de Calificación

La calificación en la **convocatoria ordinaria** de la asignatura se obtendrá como:

- Un 70% la calificación de los exámenes. La nota del examen final supondrá un 60% de la nota final en la asignatura y un 10% de la nota será la de pruebas intermedias.
- Un 30% será la nota de seguimiento, formada por trabajo práctico individual, participación en clase, pruebas rápidas durante la clase.

No hay nota mínima en el examen final de la asignatura.

Convocatoria Extraordinaria

- Un 80% la nota del examen de la convocatoria extraordinaria.
- Un 20% la nota de trabajos de carácter práctico individual.

La inasistencia a más del 15% de las horas presenciales de esta asignatura puede tener como consecuencia la imposibilidad de presentarse a la convocatoria ordinaria de esta asignatura. La asistencia a las prácticas de laboratorio es obligatoria.

RESUMEN PLAN DE LOS TRABAJOS Y CRONOGRAMA

Actividades Presenciales y No presenciales	Fecha de realización	Fecha de entrega
Prácticas de laboratorio y elaborar informe		
Lectura y estudio de contenidos teóricos		
Preparación de pruebas a realizar en tiempo de clase		
Preparación del examen final		

RESUMEN HORAS DE TRABAJO DEL ALUMNO			
HORAS PRESENCIALES			
Lección magistral	Resolución de problemas	Prácticas laboratorio	
25	5+5	10	
HORAS NO PRESENCIALES			
Trabajo autónomo sobre contenidos teóricos	Trabajo autónomo sobre contenidos prácticos	Realización de trabajos colaborativos	
45	25	20	
		CRÉDITOS ECTS:	4,5 (135 horas)

BIBLIOGRAFÍA Y RECURSOS

Bibliografía Básica

Libros de texto

- John Vacca, Managing Information Security.2nd edition Ed. Syngress. (2014).
- Michael Zalewski, The Tangled Web. A guide to securing modern web applications Ed. No Starch Press (2012).

Bibliografía Complementaria

Artículos

Attacks on SSL - A comprehensive study of BEAST, CRIME, TIME, BREACH, LUCKY 13 & RC4 biases
Pratik Guha Sarkar, Shawn Fitzgerald
https://www.nccgroup.trust/globalassets/our-research/us/whitepapers/ssl_attacks_survey.pdf

Bypassing HTTP Strict Transport Security
Jose Selvi
https://www.blackhat.com/docs/eu-14/materials/eu-14-Selvi-Bypassing-HTTP-Strict-Transport-Security-wp.pdf

SMB : Sharing more than your files
Xiaoran Wang, Sergey Gorbaty, Hormazd Billimoria, Angelo Prado, Anton Rager, Jonathan Brossard
https://www.blackhat.com/docs/us-15/materials/us-15-Brossard-SMBv2-Sharing-More-Than-Just-Your-Files-wp.pdf

BREACH: Reviving the CRIME attack
Yoel Gluck, Neal Harris and Angelo (Angel) Prado
http://breachattack.com/resources/BREACH%20-%20SSL,%20gone%20in%2030%20seconds_orig.pdf

SOME - Same Method Origin Execution
Ben Hayak
http://files.benhayak.com/Same_Origin_Method_Execution__paper.pdf

Side-Channel Leaks in Web Applications: a Reality Today, a Challenge Tomorrow
Shuo Chen, Rui Wang, XiaoFeng Wang
http://research.microsoft.com/pubs/119060/WebAppSideChannel-final.pdf

FileCry - The new age of XXE (IE + Java JDK XML Parsers)
Xiaoran Wang & Sergey Gorbaty
https://www.blackhat.com/docs/us-15/materials/us-15-Wang-FileCry-The-New-Age-Of-XXE-ie-wp.pdf

https://www.blackhat.com/docs/us-15/materials/us-15-Wang-FileCry-The-New-Age-Of-XXE-java-wp.pdf

More Tricks For Defeating SSL In Practice
Moxie Marlinspike
https://www.blackhat.com/presentations/bh-usa-09/MARLINSPIKE/BHUSA09-Marlinspike-DefeatSSL-SLIDES.pdf

Reflections on Trusting Trust
Ken Thompson
http://www.ece.cmu.edu/~ganger/712.fall02/papers/p761-thompson.pdf

Pixel Perfect Timing Attacks with HTML5
Paul Stone
http://www.contextis.com/documents/2/Browser_Timing_Attacks.pdf

Compromising the Windows Enterprise via Windows Update
Paul Stone & Alex Chapman
https://www.blackhat.com/docs/us-15/materials/us-15-Stone-WSUSpect-Compromising-Windows-Enterprise-Via-Windows-Update-wp.pdf

The Matter of Heartbleed
Zakir Durumeric, James Kasten, David Adrian, J. Alex Halderman, Michael Bailey
https://jhalderm.com/pub/papers/heartbleed-imc14.pdf

Polyglots: Crossing Origins by Crossing Formats
Jonas Magazinius, Billy Rios, Andrei Sabelfeld
http://www.cse.chalmers.se/~andrei/ccs13.pdf

BEAST - Here Come The ⊕ Ninjas
Thai Duong, Juliano Rizzo
http://core0.staticworld.net/downloads/idge/imported/article/ifw/2011/09/26/beast_duong_rizzo.pdf

This POODLE Bites: Exploiting The SSL 3.0 Fallback
Bodo Möller, Thai Duong, Krzysztof Kotowicz
https://www.openssl.org/~bodo/ssl-poodle.pdf

I Know Where You've Been: Geo-Inference Attacks via the Browser Cache
Yaoqi Jia, Xinshu Dong, Zhenkai Liang
http://w2spconf.com/2014/papers/geo_inference.pdf

Elevation of Privilege: Drawing Developers into Threat Modeling
Adam Shostack
https://www.usenix.org/system/files/conference/3gse14/3gse14-shostack.pdf

PKI Layer Cake: New Collision Attacks Against the Global X.509 Infrastructure
Dan Kaminsky
https://www.cosic.esat.kuleuven.be/publications/article-1432.pdf

Making Programs Forget: Enforcing Lifetime For Sensitive Data
Jayanthkumar Kannan, Gautam Altekar, Petros Maniatis, Byung-Gon Chun
https://www.usenix.org/legacy/events/hotos11/tech/final_files/Kannan.pdf

Why Silent Updates Boost Security
Thomas Duebendorfer, Stefan Frei
http://www.techzoom.net/Papers/Browser_Silent_Updates_%282009%29.pdf

Macaroons: Cookies with Contextual Caveats for Decentralized Authorization in the Clou
Arnar Birgisson, Joe Gibbs Politz
http://static.googleusercontent.com/media/research.google.com/en//pubs/archive/41892.pdf

Cryptography in the Web: The Case of Cryptographic Design Flaws in ASP.NET
Thai Duong, Juliano Rizzo
http://netifera.com/research/poet/PaddingOraclesEverywhereEkoparty2010.pdf

Launching Generic Attacks on iOS with Approved Third-Party Applications
Jin Han, Su Mon Kywe, Qiang Yan, Feng Bao, Robert Deng
http://www.liaiqin.com/hanjin/papers/ACNS2013Han.pdf

Jekyll∗ on iOS: When Benign Apps Become Evil
Tielei Wang, Kangjie Lu, Long Lu, Simon Chung, and Wenke Lee
http://www.cc.gatech.edu/~klu38/publications/security13.pdf

Touchjacking Attacks on Web in Android, iOS, and Windows Phone
Tongbo Luo, Xing Jin, Ajai Ananthanarayanan, and Wenliang Du
http://www.cis.syr.edu/~wedu/Research/paper/touchjacking_FPS2012.pdf

Owning Bad Guys {& Mafia} with JavaScript Botnets
Chema Alonso
https://media.blackhat.com/bh-us-12/Briefings/Alonso/BH_US_12_Alonso_Owning_Bad_Guys_WP.pdf

Incident Response Guide to the Kaminsky DNS Cache Poison Exploit
Team Cymru
https://www.team-cymru.com/ReadingRoom/Whitepapers/2008/kaminsky-cache-poison-ir.pdf

A Study of Android Application Security
William Enck, Damien Octeau, Patrick McDaniel, and Swarat Chaudhuri

http://www.cs.rice.edu/~sc40/pubs/enck-sec11.pdf

Protecting Browsers from DNS Rebinding Attacks
Collin Jackson, Adam Barth, Andrew Bortz, Dan Boneh
https://crypto.stanford.edu/dns/dns-rebinding.pdf

Clickjacking: Attacks and Defenses
Lin-Shung Huang, Alex Moshchuk, Helen J. Wang
https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final39.pdf

Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devies
Michael Becher, Felix C. Freiling
http://www.ieee-security.org/TC/SP2011/PAPERS/2011/paper007.pdf

mXSS Attacks: Attacking well-secured Web-Applications by using innerHTML Mutations
Mario Heiderich
https://cure53.de/fp170.pdf

Insertion Evasion and Denial of Service Eluding Network Intrusion Detection
Thomas H Ptacek, Timothy N. Newsham
https://sparrow.ece.cmu.edu/group/731-s08/readings/ptacek-newsham.pdf

How Unique Is Your Web Browser?
Peter Eckersley
https://panopticlick.eff.org/browser-uniqueness.pdf

Threat Modeling: Lessons from Star Wars
Adam Shostack
https://courses.cs.washington.edu/courses/cse484/14au/slides/thread-modeling.pdf