

Agenda

1. Introducción
2. Amenazas, Vulnerabilidades, Riesgos y Ataques a la Infraestructura de VoIP
3. Modelos y Estándares de Seguridad
4. Mejores Prácticas: Prevención, Protección y Mitigación
5. Recomendaciones Finales

Introducción

¿Cuántos han recibido SPAM por Skype/VoIP?

¿...y por la PSTN?

¿...en el negocio en el hogar?

¿Alguna vez se ha “caído la red”?

Mitos de la Seguridad

La tecnología es el último paso

...o cortar el cable de Internet

Sí, si nadie puede intervenir los cables.

... si te gusta la complejidad

- ❑ Inicia buscando la solución tecnológica más avanzada
- ❑ Es suficiente comprar un firewall de \$300,000 usd.
- ❑ La PSTN es 100% segura.
- ❑ NAT es estupendo

Preocupaciones en VoIP

Al implementar soluciones de VoIP la gente se preocupa principalmente por:

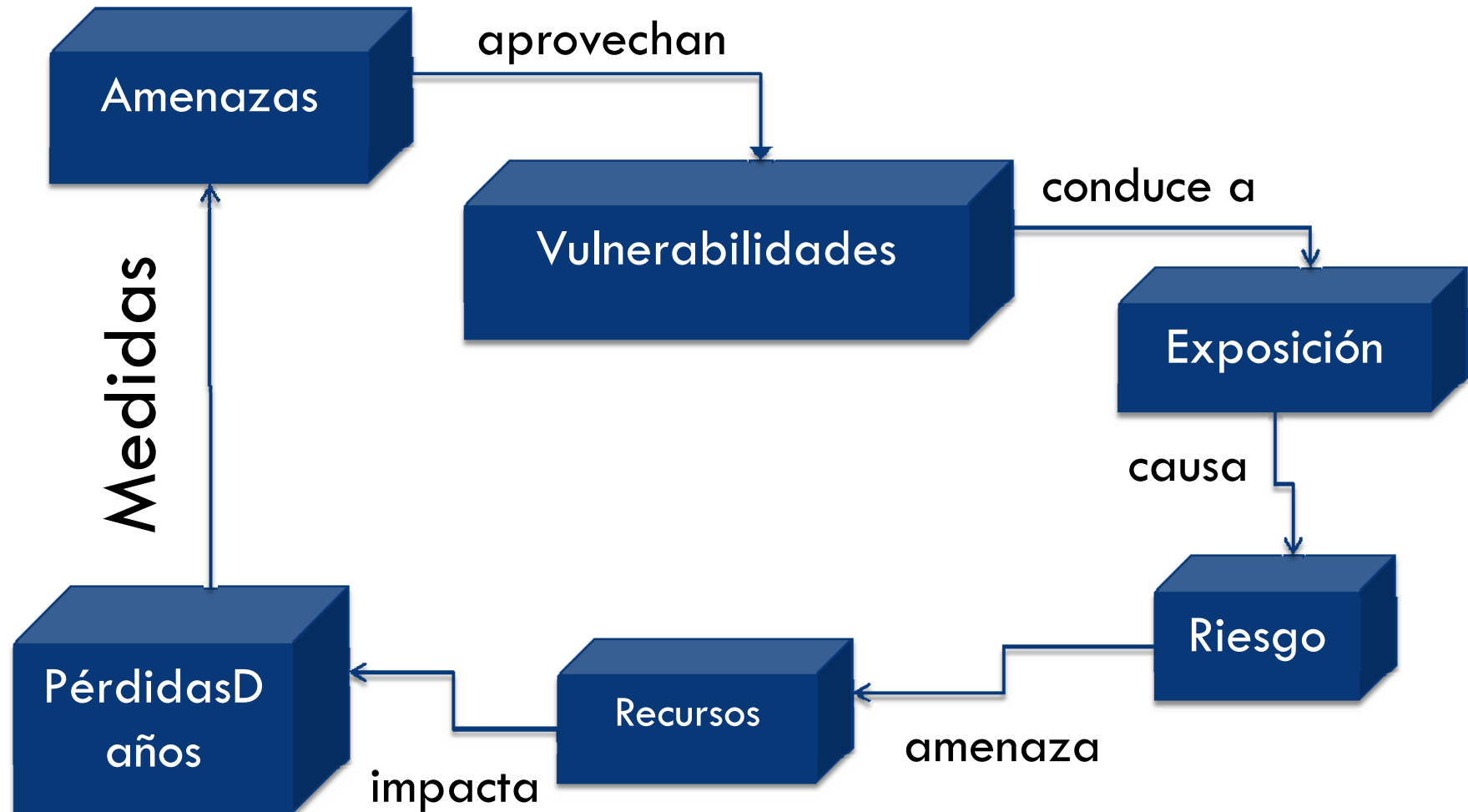
... y la Seguridad?

- ❑ Calidad de Voz
- ❑ Latencia/Jitter
- ❑ Interoperabilidad

- ❑ Ha sido ignorada hasta recientemente por “nueva” y por falta de estándares
- ❑ No solamente los ataques maliciosos amenazan sino la mala configuración.

Amenazas, Vulnerabilidades, Riesgos y Ataques

Relación de Términos



Amenazas

- Actividad que representa peligro
- Existe en diferentes formas
- Vienen de diferentes lugares
- Imposible protegerse contra todas
- Hay que protegerse contra las más probables o las más preocupantes:
 - Misión del Negocio
 - Datos (integridad confidencialidad, disponibilidad)

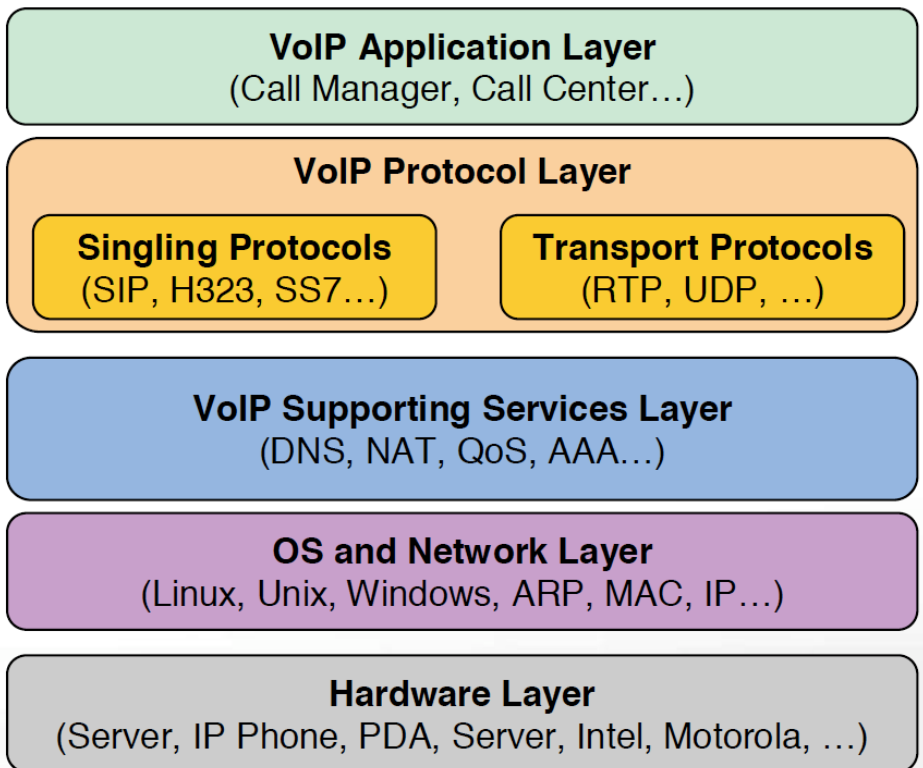
Vulnerabilidades

•Una condición, debilidad o ausencia de procedimientos de seguridad, controles técnicos, controles físicos o cualquier otro control que puede ser explotado por una vulnerabilidad.

•Se analiza típicamente en términos de controles faltantes.

•Contribuye al riesgo por que permite que una amenaza dañe al sistema.

•En VoIP los puntos de ataque, es decir las vulnerabilidades, son cientos.



Riesgos

- Potencial de daño o pérdida
- Exposición a una amenaza
- Depende de la situación y circunstancia
- Imposible de medir por completo

Falacias sobre el Riesgo

- Vulnerabilidades = Riesgo
 - ▣ La verdad: Vulnerabilidades = Vulnerabilidades
 - ▣ La evaluación de vulnerabilidad es por sí sola no identifica o cuantifica riesgo.
- Las amenazas no son un elemento de riesgo
 - ▣ La verdad: las amenazas son el elemento más importante del riesgo
- Herramientas = Medidas de seguridad
 - ▣ La verdad: Las herramientas son sólo herramientas. Muchas medidas son administrativas o combinación de herramientas y administración.
 - ▣ Las mejores medidas de seguridad se implementan en capas
- Todos los riesgos deben ser mitigados
 - ▣ La verdad: No hay que perder tiempo protegiendo basura. Es válido el concepto de “Riesgo Aceptable”.

Ataques Comunes en VoIP

- SPIT (SPam over Internet Telephony)
- DoS (Denial of Service)
 - ▣ Contra servidores o terminales
- Abuso de Servicio (fraude)
 - ▣ Utilización no autorizada o no contabilizada, identidad falsa, personificación o reproducción de sesión
- Intercepción y Modificación
 - ▣ Las conversaciones pueden ser escuchadas, la info privada puede ser robada, la señalización puede ser modificada

Modelos y Estándares de Seguridad

Primera línea de defensa: políticas y procedimientos para administración de la seguridad.

Estándares de Seguridad Informática

El más
popular...

- ISO/IEC 27002:2007
 - ▣ Antes se llamaba ISO17799
- OSSTMM
- CoBit
- SSECMM
- Common Criteria
- AICPA Trust Services

ISO/IEC 27002:2007

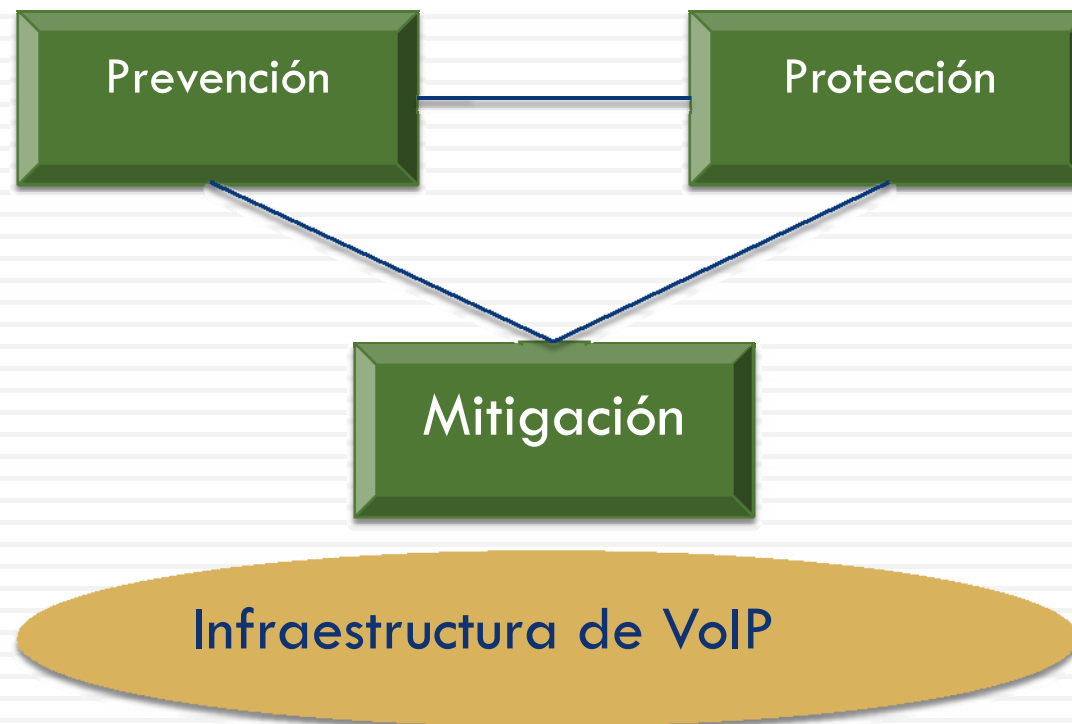
- ▣ Security Policy
- ▣ Asset Classification
- ▣ Security organization
- ▣ Personnel Security
- ▣ Computer and Network Management
- ▣ Physical and Environmental Security
- ▣ System Development and Maintenance
- ▣ Compliance
- ▣ System Access Control
- ▣ Business Continuity Planning

Modelo de las Políticas de Seguridad

ISO 27002:2007



Mejores Prácticas: Prevención, Protección y Mitigación



Prevención

- ▣ Identificar amenazas antes de que causen daño.
- ▣ Evaluar equipo de VoIP antes, durante y después de la implementación.
- ▣ Evaluar vulnerabilidades a nivel sistema.

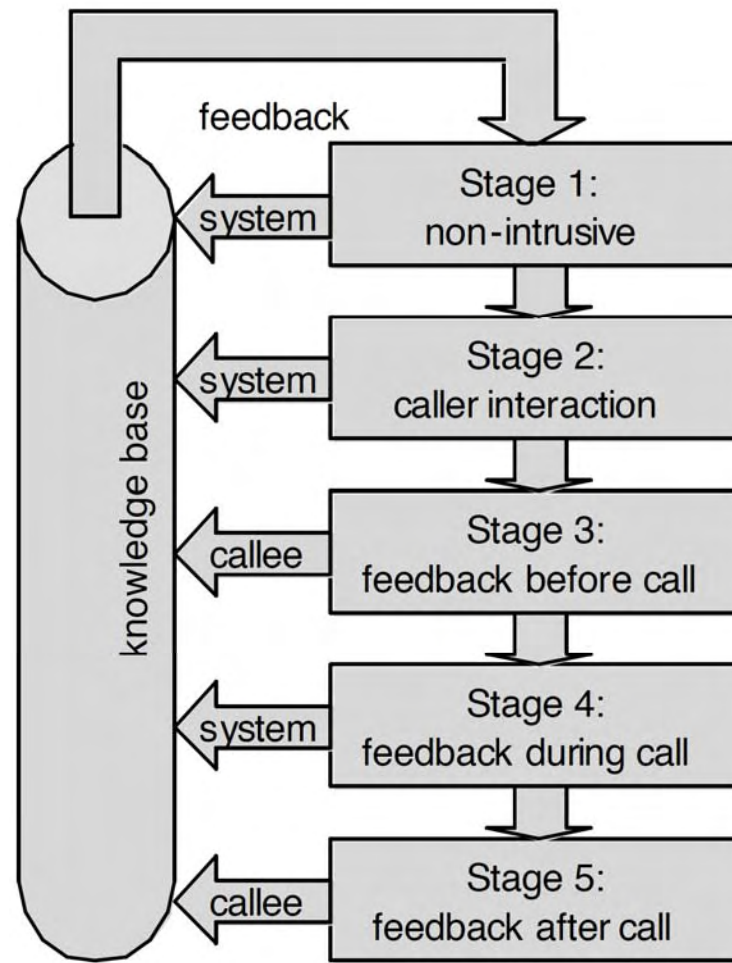
Protección

- ▣ Protección continua de los servicios VoIP contra amenazas de seguridad durante todo el ciclo de vida.
- ▣ Debe ser “VoIP aware” para disminuir el impacto en calidad y confiabilidad.
- ▣ Infraestructura multi-capas que incluya protección de la red perimetral.
- ▣ Consiste en diversos equipos de seguridad y aplicaciones hospedadas – SBCs (Session Border Controllers), IPS (Intrusion Prevention Systems) y IDS (Intrusion Detection System), Servidores AAA, Motores de Encriptación.
- ▣ Debe ser coordinada mediante una aplicación de alto nivel para mostrar una perspectiva unificada de todo el sistema VoIP a los proveedores de servicio.

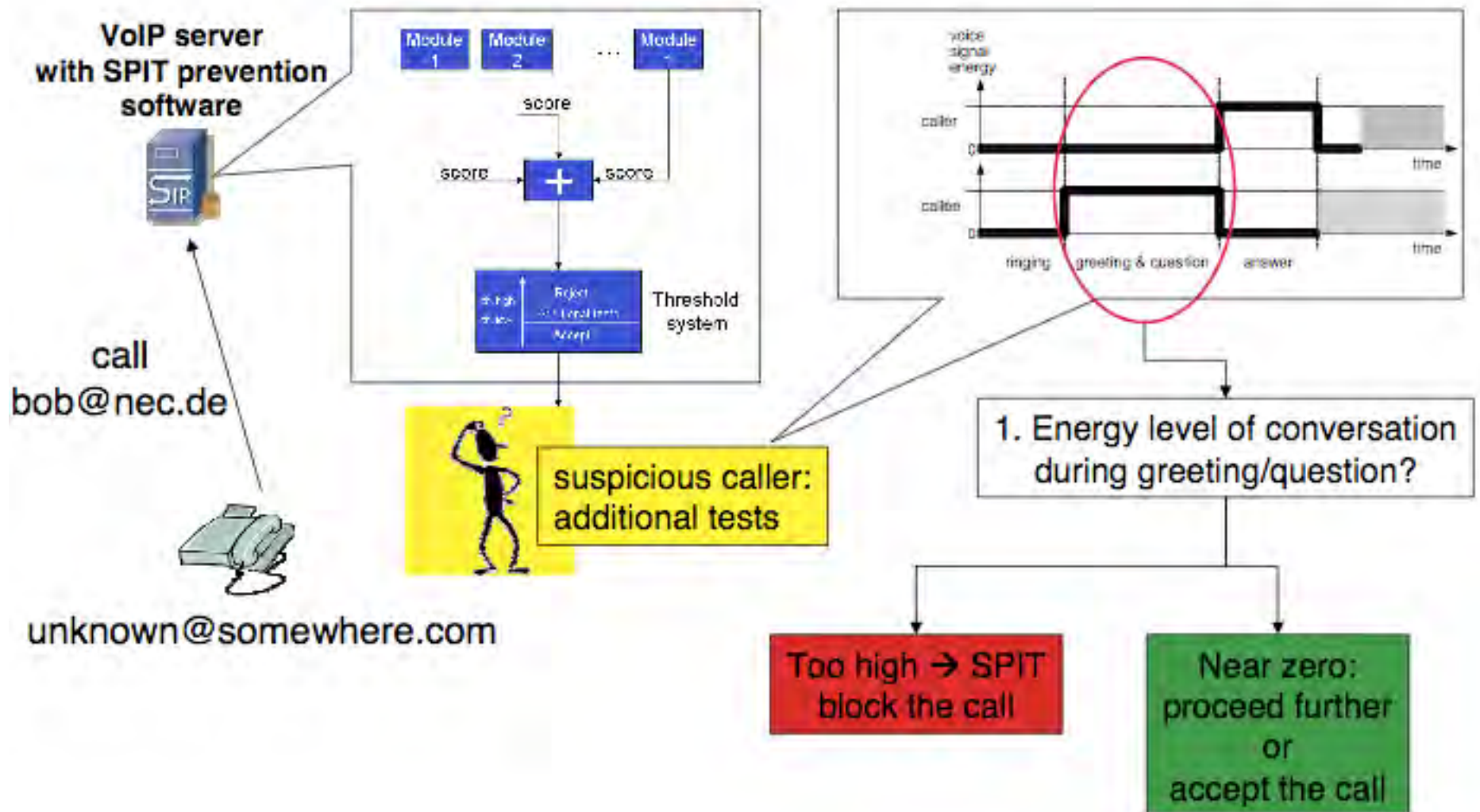
Mitigación

- Mantiene los servicios de VoIP disponibles en presencia de amenazas ya desarrollándose en la infraestructura
- **Elementos de Mitigación en VoIP**
 - ▣ **Detección:** *La amenaza se debe identificar cuanto antes usando conceptos independientes de firmas como por ejemplo detección basada en anomalías.*
 - ▣ **Correlación:** *Una vez que una amenaza se detecta se debe correlacionar con información conocida de ese dispositivo. Se requiere una tasa baja de falsos/positivos. Una base de conocimiento específica para VoIP.*
 - ▣ **Respuesta:** *Respuesta automática es la única opción. Basada en políticas. Y responder en tiempo real.*

Prevención de SPIT y DoS



Estado del Arte: PPM SPIT



Criptografía

- El arte de enviar mensajes secretos
- Larga historia: emperadores romanos
- Algo común: papelitos en la escuela
- El principio:

ALICE envía: 0 1 0 0 1 1 0 1

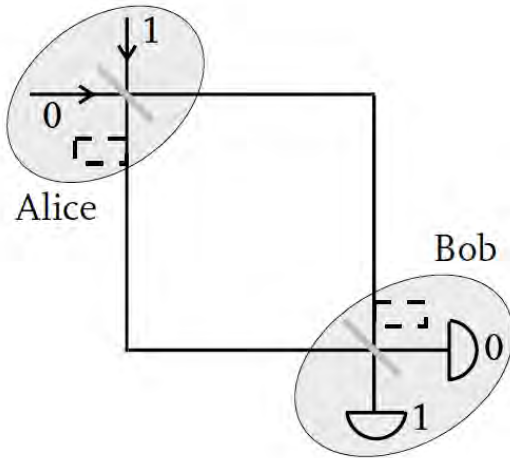
Llave secreta: 1 0 0 1 1 0 0 1

BOB de cifra: 0 0 1 0 1 0 1 1

Criptografía

- **El problema:** distribución de llaves secretas
- **La solución actual:** llaves largas y complicadas matemáticamente
- **La solución a la larga:** usar física en vez de matemáticas... Criptografía Cuántica

Distribución Cuántica de Llaves



- Alice envía algunas partículas a Bob.

Alice			Bob		
Particle #	Bit (input)	Extension	Particle #	Bit (output)	Extension
1	0	Yes	1	0	Yes
2	0	No	2	0	Yes
3	1	No	3	1	No
4	0	No	4	1	Yes
5	1	No	5	1	No
6	1	Yes	6	0	No

- Alice y Bob intercambian públicamente el resultado de la última columna
- Alice y Bob verifican algunos de los bits: los otros forman la llave

Cuántica:

Si ambos extienden o ninguno, cuando Alice envía 1, Bob recibe 1 e igual con 0.

Si uno de los dos extiende, BOB tiene 50% de probabilidad de recibir 0 o 1.

Recomendaciones Finales

- Políticas y Procesos clave:
 - ▣ Preparar
 - ▣ Planear
 - ▣ Diseñar
 - ▣ Implementar
 - ▣ Operar
 - ▣ Optimizar

Recomendaciones Finales

- Proteger tráfico de VoIP
 - ▣ Encriptar
 - ▣ Configurar apropiadamente firewalls
 - ▣ Segmentar tráfico de voz y de datos
 - ▣ Usar servidores proxy delante de los firewalls
 - ▣ Asegurar los IP-PBX's